IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

RIGHTQUESTION, LLC, **Plaintiff,** **v.** **SAMSUNG ELECTRONICS CO., LTD., AND SAMSUNG ELECTRONICS AMERICA, INC.,** **Defendants.**	**Civil Action No. 2:21-cv-00238** **JURY TRIAL**

RIGHTQUESTION'S ORIGINAL COMPLAINT

Plaintiff RightQuestion, LLC, ("RightQuestion") files this Complaint for Patent Infringement against Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung"), and alleges as follows:

NATURE OF ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

2. Samsung has infringed and continues to infringe at least one claim of U.S. Patent Nos. 10,824,696 and 10,929,512 (collectively the "patents-in-suit"). *See* Exs. 1 and 2.

3. Samsung infringes directly, literally and/or by the doctrine of equivalents, contributes to the infringement of, and/or induces infringement of the patents-in-suit by making, using, selling, offering for sale, and/or importing into the United States products that incorporate RightQuestion's patented authentication technology.

4. RightQuestion seeks damages and other relief for Samsung's infringement of the RightQuestion's patented technology.

PARTIES

5. Plaintiff RightQuestion, LLC, is a California limited liability company having its principal place of business at 118 Ramona Road, Portola Valley, CA 94028.

6. Defendant Samsung Electronics Co., Ltd. ("SEC") is a corporation organized and existing under the laws of the Republic of Korea with a principal place of business at 129 Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-Do, Korea 443-742.

7. Defendant Samsung Electronics America, Inc. ("SEA") is a New York corporation having a principal place of business at 85 Challenger Road, Ridgefield Park, New Jersey 07660, and it is a wholly owned subsidiary of SEC.

8. On information and belief, SEA imports into the United States and sells in the United States, including in this district, mobile devices.

9. The patents-in-suit are infringed through various Samsung mobile devices. Defendants SEC and SEA are related entities that work in concert to design, manufacture, import, distribute, and/or sell those infringing devices.

JURISDICTION AND VENUE

10. This is an action for patent infringement under the patent laws of the United States, 35 U.S.C. § 271. This Court has jurisdiction on federal question claims pursuant to 28 U.S.C. §§ 1331 and 1338(a).

11. This Court has personal jurisdiction over both Samsung entities (SEC and SEA). Samsung has continuous and systematic business contacts with the State of Texas. Samsung, directly or through subsidiaries or intermediaries, conducts its business extensively throughout Texas, by shipping, distributing, offering for sale, selling, and advertising its products and/or services in the State of Texas and the Eastern District of Texas. Samsung, directly and through subsidiaries or intermediaries, has purposefully and voluntarily placed one or more of its infringing

products and/or services into the stream of commerce with the intention and expectation that they will be purchased and used by consumers in the Eastern District of Texas. These products and/or services have been and continue to be purchased and used by consumers in the Eastern District of Texas. In addition, on information and belief, SEA's business operations relating to mobile devices, which are devices accused of infringement in this Action, are conducted at its Eastern District of Texas facility

12. Venue is proper in this judicial district under 28 U.S.C. §§ 1391 and 1400(b). With respect to SEA, venue is proper in this district under 28 U.S.C. §1400(b) because SEA has a regular and established place of business in this district and has committed acts of infringement in this district. On information and belief, SEA's business operations relating to mobile devices, like cell phones, which are devices accused of infringement in this Action, are conducted at its Texas facility located within the Eastern District of Texas located at 6625 Excellence Way, Plano, Texas 75023. Defendant SEA also employs full-time personnel, such as engineers and senior managers in this district. On information and belief, Samsung's business operations relating to mobile devices are conducted at the SEA facility located in this district. Defendant SEA has also committed acts of infringement in this district by commercializing, marketing, selling, distributing, and servicing certain Samsung-branded devices, including but not limited to cell phones, which are devices RightQuestion accuses of infringement in this Action.

13. With respect to SEC, a Korean company, venue is proper because suits against foreign entitles are proper in any judicial district.

14. In other patent infringement matters involving Samsung's mobile devices, such as *Ericsson Inc., v. Samsung Electronics Co., Ltd. et al.*, Samsung has admitted that for patent infringement actions involving mobile devices, venue is proper in this District and that this Court

may exercise personal jurisdiction over both SEC and SEA. *See Ericsson Inc., v. Samsung Electronics Co., Ltd. et al.*, No. 2:21-cv-00010-JRG, Defendants' Answer and Counterclaims at ¶¶ 7-8, Dkt. No. 7 (EDTX Feb. 4, 2021); *see also Clear Imaging Research, LLC v. Samsung Electronics Co., Ltd. et al.*, No. 2:19-cv-326, Samsung Defendants' Answer at ¶¶ 7-8, Dkt. No. 23 (EDTX Jan. 22, 2020); *R2 Solutions LLC v. Samsung Electronics America, Inc.*, No. 4:21-cv-00089, Defendant Samsung Electronics America, Inc.'s Answer at ¶¶ 5-8, Dkt. No 14 (Apr. 19, 2021).

FACTUAL BACKGROUND

15. RightQuestion was founded by Dr. Markus Jakobsson with a focus on user authentication and security. Dr. Jakobsson is a preeminent security researcher with interests in applied security, ranging from device security to user interfaces. He is one of the main contributors to the understanding of phishing and crimeware and currently focuses his efforts on social engineering, human aspects of security, and mobile security. Dr. Jakobsson has published a collection of books and over one hundred peer-reviewed conference and journal articles related to user data security.[1]

16. Dr. Jakobsson's passion for user security started while pursuing a degree in computer engineering from the Lund Institute of Technology in Sweden. During his studies, Dr. Jakobsson focused on automated controls and robotics; however, Dr. Jakobsson started to notice that the main problem in the field of automated controls related to getting guided missiles to a target. Feeling dismayed about being involved with weapons, Dr. Jakobsson began looking for a path where the main application was not guiding a missile to destroy but rather protecting or defending something.

[1] More information on Dr. Jakobsson can be found at https://www.markus-jakobsson.com/.

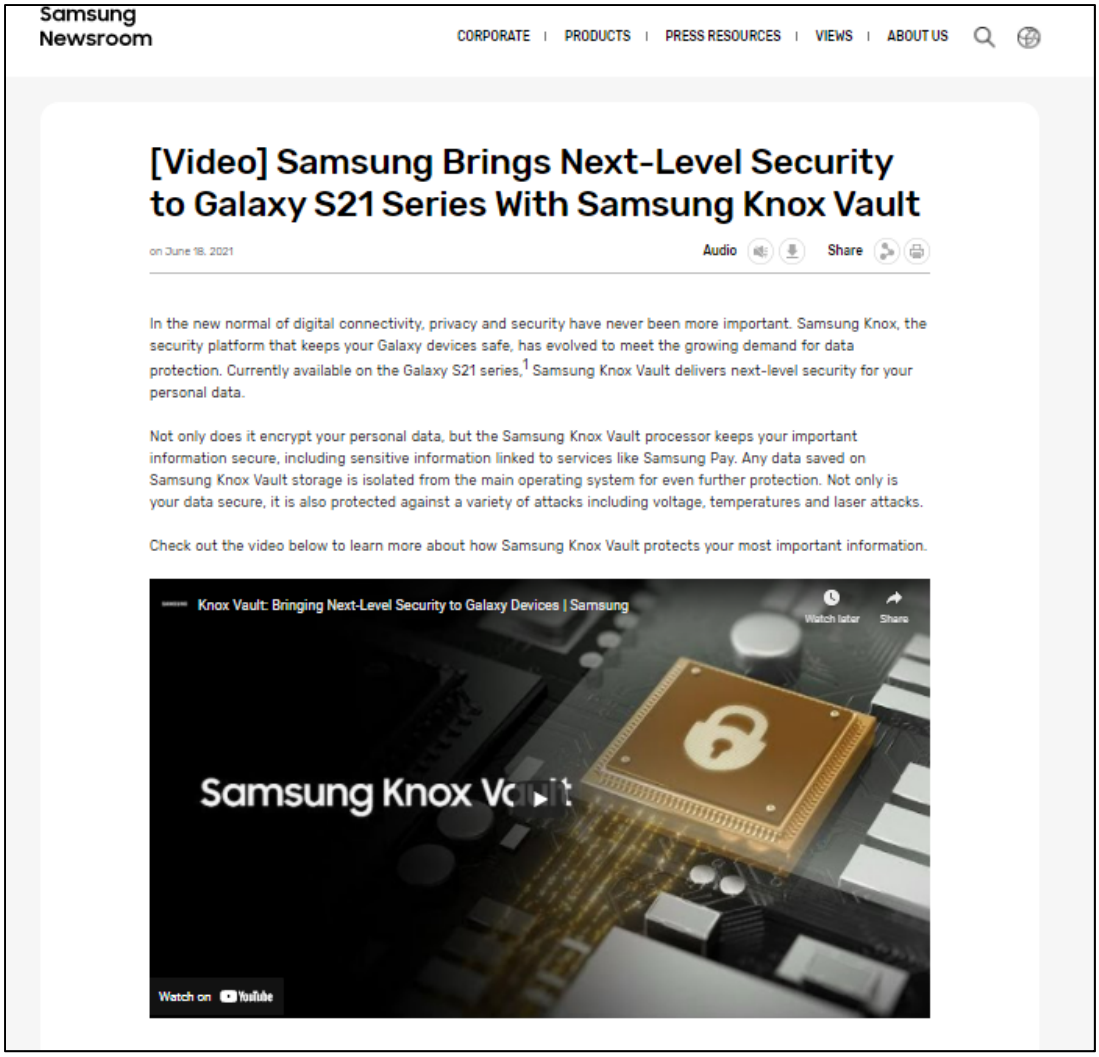
17. With this in mind, Dr. Jakobsson became interested in computer security, which at its very core is about protecting information and resources. After he completed his computer science graduate studies at the U.C. San Diego, Dr. Jakobsson realized that most of the security problems revolved around the divide between a user's security preference and the usability/user experience of a given security feature. For example, a user may prefer to use safe security practices such as complex usernames and passwords; however, the tedious experience of implementing and using a complex password combination may lead users to use less secure, simple passwords or reuse old passwords.

18. One way to address this issue is to use a password manager secured by a user's biometrics. Users are more inclined to use stronger, complex passwords when storing and retrieving the password is as simple as scanning a biometric—such as a fingerprint or face scan—when prompted by a device. However, Dr. Jakobsson knew that despite the advantages of biometrics for storing and securing passwords, if biometric features were not properly deployed, they could be more insecure than traditional passwords.[2] For example, if a user sends biometrics from a device with a biometric reader (like a phone or tablet) to a different device (like a server) for verification, the user is sending their most sensitive data over a network that is out of their control and vulnerable to malicious actors. On the other hand, if a user uses a device with the biometric reader to scan and verify a biometric, the user is storing their most sensitive data—such as their biometrics—in the device's main storage and leaving that data vulnerable to security breaches and malware. Dr. Jakobsson determined that the correct way to deal with this was to create a secure portion of a device where at least some processing of the user's most sensitive data would be done. This solution eliminates the network security issue because that data is never sent

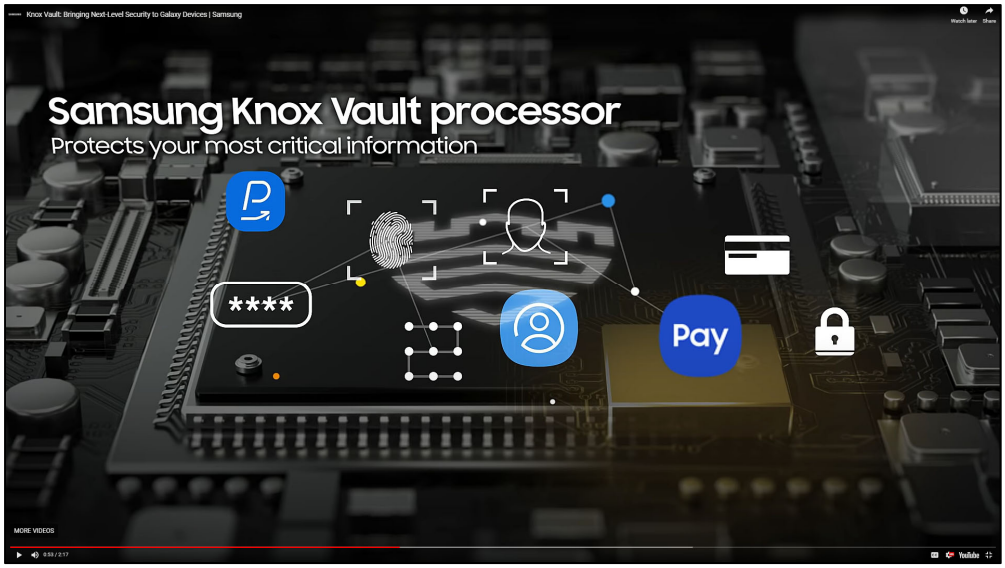
[2] Unlike a password, a compromised biometric cannot be changed.

over an unprotected network, and it does not expose the data to breaches and other forms of malware.

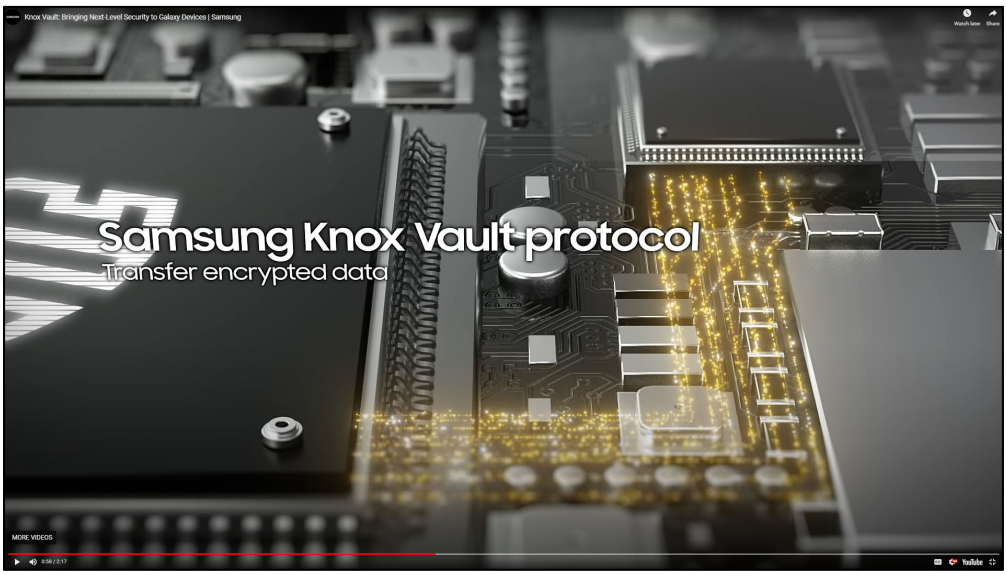
19. As set forth below, having fallen behind its competitors, Samsung turned to RightQuestion's patented technology to improve the user security experience in many of its recent flagship mobile devices. For example, Samsung relies on RightQuestion's patented technology to enable Knox Vault on the Galaxy S21. Knox Vault comprises a "secure processor," "secure memory," and "integrated software" "to manage and protect the most critical information: PINs, passwords, biometrics, digital certificates, cryptographic keys and other sensitive information." David Thomson, *Understanding Samsung Knox Vault: Protecting the data that matters most*, SAMSUNG NEWSROOM U.S. (Mar. 3, 2021), https://news.samsung.com/us/understanding-samsung-knox-vault-protecting-data-matters-most/.



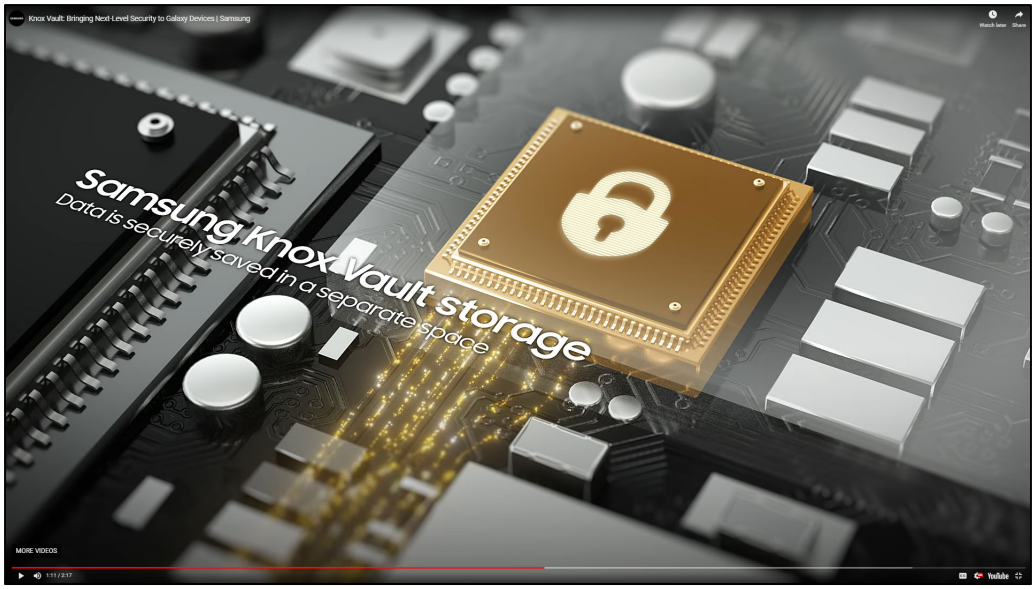
Samsung Brings Next-Level Security to Galaxy S21 Series with Samsung Knox Vault, SAMSUNG NEWSROOM (June 18, 2021), https://news.samsung.com/global/samsung-brings-next-level-security-to-galaxy-devices-with-samsung-knox-vault (last accessed June 28, 2021).


Knox Vault: Bringing Next-Level Security to Galaxy Devices | Samsung
Samsung Knox Vault processor
Protects your most critical information
****
Pay
MORE VIDEOS

[. . .]


Knox Vault: Bringing Next-Level Security to Galaxy Devices | Samsung
Samsung Knox Vault protocol
Transfer encrypted data
MORE VIDEOS

[. . .]



Samsung, *Knox Vault: Bringing Next-Level Security to Galaxy Devices| Samsung*, YOUTUBE (June 22, 2021), https://www.youtube.com/watch?v=cSBZXC4hel8.

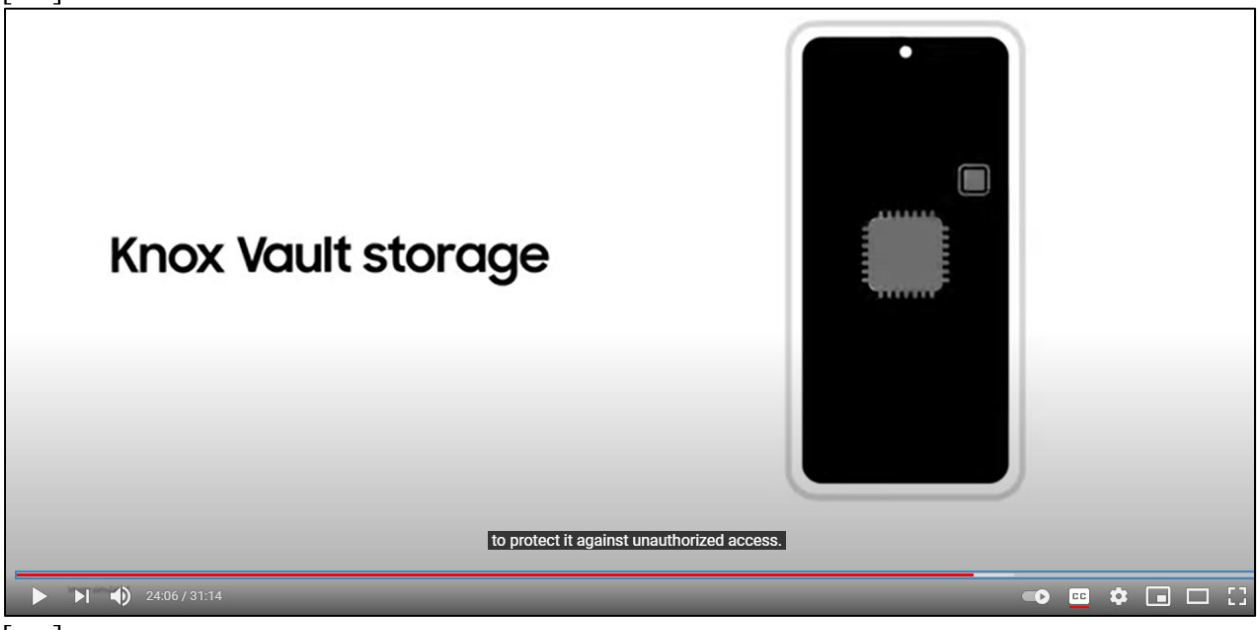
20. Samsung touts these infringing security features as selling points of its devices. For example, Samsung discussed the security features enabled by the patented inventions during the live Galaxy S21 device announcement.

Samsung, *Galaxy Unpacked January 2021: Official Replay l Samsung*, YOUTUBE (Jan. 14, 2021), https://www.youtube.com/watch?v=TD_BZN0bn_U&t=1s.

21. Similarly, during Mobile World Congress 2021, Samsung spent roughly ten minutes of its thirty minute presentation discussing the security features of its Galaxy devices, like

Knox Vault. *See* Samsung, *Galaxy MWC Virtual Event Livestream | Samsung*, YOUTUBE (June 28, 2021), https://www.youtube.com/watch?v=LfSZvIqYDSM (discussing Galaxy security features from 17:50-28:40).

[. . .]



[. . .]

Id.

22. Samsung has also published customer-oriented articles that describe the features enabled by RightQuestion's patented technology as one of the "10 reasons to upgrade to the [Samsung] Galaxy S21."

9. Defense-grade Knox security

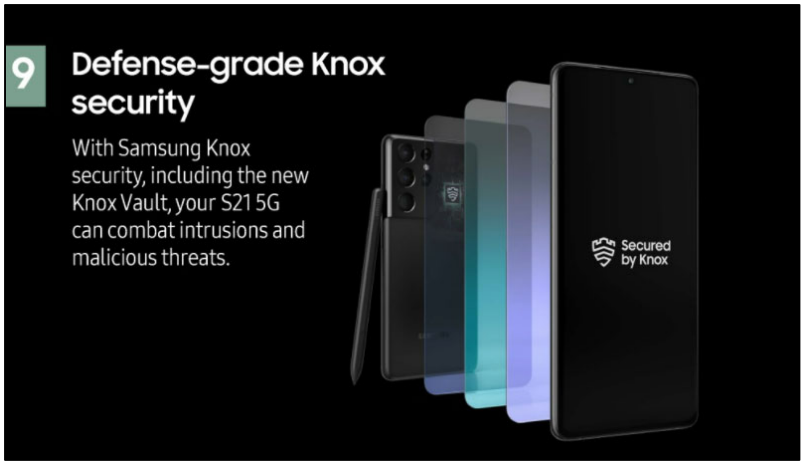
Samsung has always been at the forefront of mobile device security. The Galaxy S21 is no different, thanks to Samsung Knox, a defense-grade solution for keeping your work and your business protected from the chip up. Knox defends your S21 from intrusions, malware and other malicious threats. The S21 devices also introduce Knox Vault, which combines tamper-resistant secure memory with our secure processor for an additional layer of protection. This advanced security architecture keeps your data — including your Blockchain private key, Samsung Pay credentials and more — out of unauthorized hands.

10. Your private data stays private

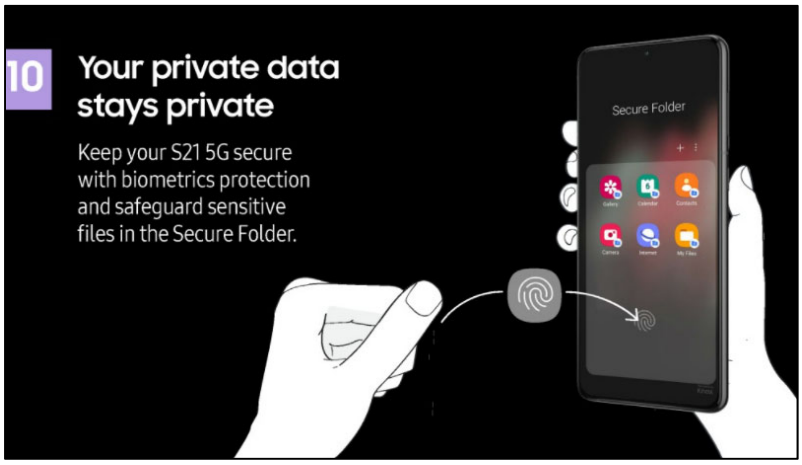
If you want to take your Galaxy S21's security one step further, you can use the device's built-in biometrics capabilities, protected by Samsung Knox. This makes accessing your device convenient but highly secure. For your most sensitive data, S21 devices include a Secure Folder feature, which adds an extra level of protection. You can also take advantage of Samsung Pass, another security tool that lets you access your saved passwords with a quick fingerprint scan.

The Galaxy S21, S21+ and S21 Ultra 5G offer a new way to work and collaborate — with natively integrated productivity apps, wireless Samsung DeX technology, Knox Vault and powerful hardware — ideal for the modern workday.

[. . .]



[. . .]



Michael Archambault, *10 Reasons to Upgrade to the Galaxy S21*, SAMSUNG INSIGHTS (Jan. 14, 2021), https://insights.samsung.com/2021/01/14/10-reasons-to-upgrade-to-the-galaxy-s21/.

23. By building its products and related services on RightQuestion's patented technologies, Samsung infringes directly, literally, and/or by the doctrine of equivalents, and/or induces infringement of the patents-in-suit by making, using, selling, offering for sale, and/or importing into the United States the Accused Products (defined below). This has caused, and continues to cause, substantial and irreparable harm to RightQuestion.

THE RIGHTQUESTION PATENTS

A. U.S. Patent No. 10,824,696

24. On November 3, 2020, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 10,824,696 ("the '696 Patent"), entitled "Authentication Translation," to inventor Bjorn Markus Jakobsson. RightQuestion owns all rights to the '696 Patent necessary to bring this action. A true and correct copy of the '696 Patent is attached hereto as Exhibit 1 and incorporated herein by reference.

25. The '696 Patent concerns systems and methods for authentication translation. As the patent explains, previous authentication techniques made "[p]roviding credentials to a service, whether via a mobile or other device . . . a tedious experience for a user." '696 Patent at 1:30-31. Because the experience was so tedious, users would "often engage in practices such as password re-use, and/or the selection of poor-quality passwords, which render their credentials less secure against attacks." *Id*. at 1:33-35. Thus, "improvements in authentication techniques [were] desirable." *Id*. at 1:35-37.

26. The inventions described in the claims of the '696 Patent address these shortcomings and make it more likely that a user will engage in secure practices. The '696 Patent discloses novel methods and systems where "users need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an 'authentication translator' via an appropriate technique, and the authentication translator will provide the appropriate credentials to the implicated service on the user's behalf." *Id*. at 2:59-64. By doing this, the system promotes better user security practices by making using complex passwords easier for the user.

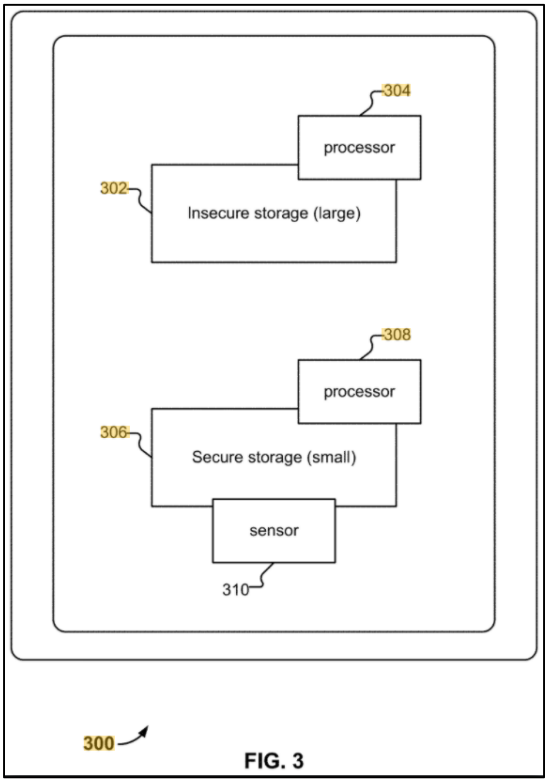
27. As the '696 patent discloses, the process begins "when a request to access a resource is received." *Id* at 6:16-17. For example, suppose "[the user] wishes to sign into [a] social

networking website." *Id*. at 6:18-19. "[The user] directs [their] web browser . . . to the social networking website." *Id*. at 6:19-21. An "[a]uthentication translator module **132** recognizes, from the context of [the user's] actions (e.g., that [the user] is attempting to access site **120** with [their] browser) that [the user] would like to access a particular resource." *Id*. at 6:21-24 (emphasis in original). The authentication translator module may then prompt "[the user] (e.g., by a popup message or via a sound) to provide biometric information (e.g., to use the integrated fingerprint reader on [the user's device])." *Id*. at 6:24-27.

28. Once a biometric has been supplied by the user, the supplied biometric data is compared "to the templates stored on [the user's device]." *Id*. at 6:35-36. "If a suitable match is found. . . the username and password for the website, as stored in a vault, such as vault **220**, are retrieved from the vault" and provided to the resource. *Id*. at 6:36-42 (emphasis in original). In the '696 Patent specification, biometrics include but are not limited to fingerprints, "facial recognition, voiceprints, or retina scan technology." *Id*. at 3:24-25; *Id*. at 3:14-15.

29. To keep the user's biometrics secure, one embodiment of the '696 Patent discloses a device with "a large and insecure storage **302** attached to a fast processor **304**, and a smaller but secure storage **306** attached to a dedicated processor **308** and a sensor **310** (e.g., a camera or a fingerprint reader)." *Id*. at 3:63-67 (emphasis in original); *see also id.* at Fig. 3 (reproduced below). The "[u]sers (and applications) can read from and write to the insecure storage area." *Id*. at 3:67-4:4. Data such as authentication information and biometrics can be stored in the secure storage. *Id*. at 3:59-61. "However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API." *Id*. at 4:1-4.

30. Figure 3 of the '696 Patent depicts a device with large and insecure storage attached to a fast processor, a smaller but secure storage attached to a dedicated processor, and a sensor in accordance with an embodiment of the inventions.



Id. at Fig. 3.

31. Further enhancing the user authentication experience and promoting better security practices, the '696 Patent also discloses a safe and convenient way of wiping a device. *See id.* at 8:5-18. For example, "user's authentication information (e.g., templates) can be used both to 'unshare' previously shared devices (e.g., where [multiple users] have user profiles on [a] shared [device]), and to avoid that criminals with physical component access to lost devices gain access to templates and vault contents." *Id*. at 8:10-15.

32. The benefits discussed in the '696 Patent specification are also reflected in the claims. *See, e.g.*, *id.* at Claim 1. Accordingly, the claims of the '696 Patent recite one or more inventive concepts rooted in computerized technology and overcome technical problems in that

field. A person of ordinary skill in the art reading the '696 Patent and its claims would understand that the patent's disclosure and claims are drawn to solving specific, technical problems arising in authentication systems/methods and provide for advancements in the field that were not routine, well-understood or conventional. Accordingly, each claim of the '696 Patent recites a combination of elements sufficient to ensure that the claim in practice amounts to significantly more than a patent claiming an abstract concept. A person of ordinary skill in the art would understand that the ordered combination of claim elements is inventive. Further, the claimed improvements over prior art authentication systems are concrete and improve the capabilities of existing authentication translation systems/methods.

33. A person of ordinary skill in the art reviewing the specification of the '696 Patent would understand that the inventors had possession of the claimed subject matter and would know how to practice the claimed invention without undue experimentation.

B. U.S. Patent No. 10,929,512

34. On February 23, 2021, the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 10,929,512 ("the '512 Patent"), entitled "Authentication Translation," to inventor Bjorn Markus Jakobsson. RightQuestion owns all rights to the '512 Patent necessary to bring this action. A true and correct copy of the '512 Patent is attached hereto as Exhibit 2 and incorporated herein by reference.

35. The '512 Patent concerns systems and methods for authentication translation. As the patent explains previous authentication techniques made "[p]roviding credentials to a service, whether via a mobile or other device . . . a tedious experience for a user." '512 Patent at 1:35-37. Because the experience was so tedious users would "often engage in practices such as password re-use, and/or the selection of poor-quality passwords, which render their credentials less secure

against attacks." *Id*. at 1:38-40. Thus, "improvements in authentication techniques [were] desirable." *Id*. at 1:40-42.

36. The '512 Patent addresses these shortcomings by disclosing novel authentication systems and methods. The '512 Patent discloses a methods and systems where "users need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an 'authentication translator' via an appropriate technique, and the authentication translator will provide the appropriate credentials to the implicated service on the user's behalf." *Id*. at 2:63-3:1. By doing this, the system promotes better user security practices by making using complex passwords easier for the user.

37. As the '512 patent discloses, the process begins "when a request to access a resource is received, as is an authentication input." *Id* at 6:20-21. For example, suppose "[the user] wishes to sign into social networking website." *Id*. at 6:22-23. "[The user] directs [their] web browser . . . to the social networking website." *Id*. at 6:23-25. The "Authentication translator module **132** recognizes, from the context of [the user's] actions (e.g., that [the user] is attempting to access site **120** with [their] browser) that [the user] would like to access a particular resource (emphasis in original). The authentication translator module may then prompt "[the user] (e.g., by a popup message or via a sound) to provide biometric information (e.g., to use the integrated fingerprint reader on [the user's device]). *Id*. at 6:25-31.

38. Once a biometric has been supplied by the user, the supplied biometric data is compared "to the templates stored on [the user's device]." *Id*. at 6:39-40. "If a suitable match is found. . . the username and password for the website, as stored in a vault, such as vault **220**, are retrieved from the vault" and provided to the resource. *Id*. at 6:40-46 (emphasis in original). In the

'512 Patent specification, biometrics include but are not limited to fingerprints, "facial recognition, voiceprints, or retina scan technology." *Id*. at 3:28-29; 3:18-19.

39. To keep the user's biometrics secure, the '512 discloses a device with "a large and insecure storage **302** attached to a fast processor **304**, and a smaller but secure storage **306** attached to a dedicated processor **308** and a sensor **310** (e.g., a camera or a fingerprint reader)." *Id*. at 3:67-4:4 (emphasis in original); *see also id.* at Fig. 3 (reproduced below). The "Users (and applications) can read from and write to the insecure storage area." *Id*. at 4:4-5. Data such as authentication information and biometrics can be stored in the secure storage. *Id*. at 3:63-65. "However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API." *Id*. at 4:5-8.

40. Figure 3 of the '512 Patent, which depicts a device with large and insecure storage attached to a fast processor, and a smaller but secure storage attached to a dedicated processor and a sensor in accordance with an embodiment of the inventions, is reproduced below.

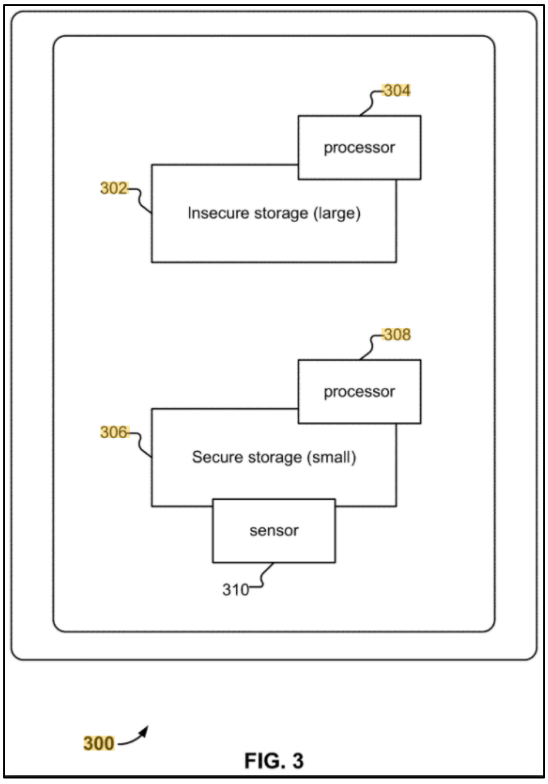


FIG. 3

Id. at Fig. 3.

41. Further enhancing the user authentication experience and promoting better security practices across multiple devices, the ’512 Patent also discloses uploading a secure back up of the records stored in the secure storage to a cloud storage service. *Id*. at 7:55-8:8. “The cloud storage service **140** is configured to accept backups from multiple devices associated with a single account, and synchronize the updates so that all devices get automatically refreshed.” *Id*. at 7:56-59 (emphasis in original). This allows a user to access and synchronize authentication information across multiple devices, *id*. at 7:59-62, further reducing the tedious experience of using complex passwords.

42. These advances are also reflected in the claims. *See, e.g.*, *id.* at Claim 1. Accordingly, the claims of the ’512 Patent recite one or more inventive concepts rooted in computerized technology and overcome technical problems in that field. A person of ordinary skill in the art reading the ’512 Patent and its claims would understand that the patent’s disclosure and

claims are drawn to solving specific, technical problems arising in authentication systems/methods and provide for advancements in the field that were not routine, well-understood or conventional. Accordingly, each claim of the '512 Patent recites a combination of elements sufficient to ensure that the claim in practice amounts to significantly more than a patent claiming an abstract concept. A person of ordinary skill in the art would understand that the ordered combination of claim elements is inventive. Further, the claimed improvements over prior art authentication systems are concrete and improve the capabilities of existing authentication translation systems/methods.

43. A person of ordinary skill in the art reviewing the specification of the '512 Patent would understand that the inventors had possession of the claimed subject matter and would know how to practice the claimed invention without undue experimentation.

CLAIMS FOR PATENT INFRINGEMENT

44. The allegations provided below are exemplary and without prejudice to RightQuestion's infringement contentions provided pursuant to the Court's scheduling order and local rules. RightQuestion's claim construction contentions regarding the meaning and scope of the claim terms will be provided under the Court's scheduling order and local rules. As detailed below, each element of at least one claim of each of the patents-in-suit is literally present in the accused products. To the extent that any element is not literally present, each such element is present under the doctrine of equivalents. RightQuestion's analysis below should not be taken as an admission that the preamble for any claim is limiting. While publicly available information is cited below, RightQuestion may rely on other forms of evidence to show infringement.

45. The Accused Products for the '696 and '512 Patents include, but are not limited to, Samsung smartphones, like the Galaxy S20 and S21 Series,[3] Galaxy Note 20 Series, Galaxy Fold

[3] The Accused Products also include variants of the names Galaxy devices like the S21 "Ultra."'

2, S9 Series, S10 Series, Note 10 Series, Z-Flip, and Fold 1, and other Samsung devices that implement the claimed inventions.

46. On information and belief, the Samsung Galaxy S9 Series, S10 Series, Note 10 Series, Z-Flip, and Fold 1 devices include a secure co-processor and secure storage.[4]

47. Identification of the accused products will be provided in plaintiff's infringement contentions pursuant to the Court's scheduling order and local rules. Samsung imports into the United States, uses, makes, offers for sale, and sells in the United States the accused products.

COUNT I: PATENT INFRINGEMENT OF THE '696 PATENT

48. RightQuestion incorporates by reference the preceding paragraphs as if fully stated herein.

49. Samsung has been and is now directly infringing and/or indirectly infringing the '696 Patent by way of inducement and/or contributory infringement, literally and/or under the Doctrine of Equivalents, in violation of 35 U.S.C. § 271, including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least '696 accused products. Samsung derives revenue from the activities relating to the '696 accused products. As explained below, these products are covered by one or more claims of the '696 Patent, including but not limited to claims 1-8, 10, 11, 13-21, 23, 24, 26, and 27.

[4] The Galaxy S9 uses the Qualcomm Snapdragon 845. SAMSUNG GALAXY S9, https://www.qualcomm.com/snapdragon/smartphones/samsung-galaxy-s9 (last accessed June 28, 2021). The Galaxy S10, Note 10, Z-Flip, and Fold 1 use the Qualcomm 855 processor. *See, e.g.,* SAMSUNG GALAXY S10, https://www.qualcomm.com/snapdragon/smartphones/samsung-galaxy-s10 (last accessed June 28, 2021); SAMSUNG GALAXY Z FLIP, https://www.qualcomm.com/snapdragon/samsung-galaxy-z-flip (last accessed June 28, 2021). The Qualcomm Snapdragon 845/855 has a Secure Processing Unit. Qualcomm, *Qualcomm Snapdragon 845 Mobile Platform Introduces New, Innovative Architectures for Artificial Intelligence and Immersion* (Dec. 6, 2017), https://www.qualcomm.com/news/releases/2017/12/06/qualcomm-snapdragon-845-mobile-platform-introduces-new-innovative (last accessed June 28, 2021).

50. For example, claim 1 of the '696 patent is reproduced below:

1. A system, comprising:

a first processor configured to:

based at least in part on a request from a user to access an external resource, communicate with a second processor using a restricted interface, wherein the second processor is configured to access at least one record stored at least in part in a secure storage;

wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:

a biometric template; and

a credential comprising at least one of a password, a cookie, or a cryptographic key;

in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, and wherein the biometric input is received subsequent to presenting of a prompt;

establish a connection with the external resource;

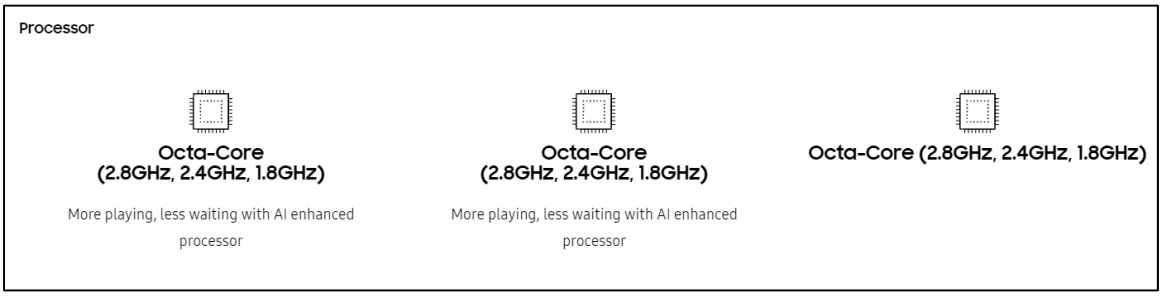
facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and

facilitate wiping of at least a portion of the at least one record; and

a memory coupled to the first processor and configured to provide the first processor with instructions.

51. As a non-limiting example, the Samsung Accused Products are systems comprising a first processor of a first device, wherein the first processor is configured to perform the limitations below. This is supported by the exemplary evidence below

[. . .]

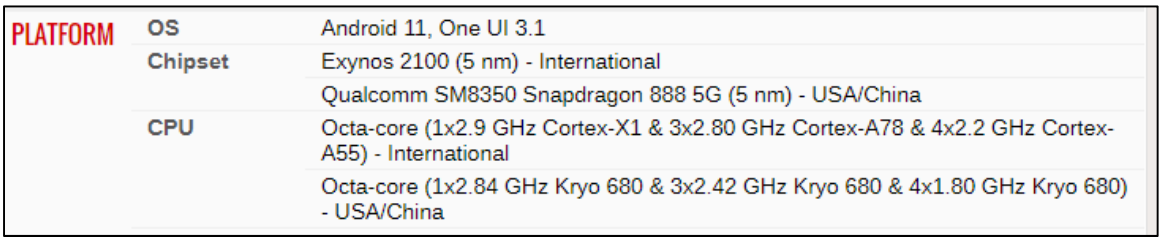


HOW THE SAMSUNG S20 FE 5G COMPARES, https://www.samsung.com/us/mobile/galaxy-s20-5g/compare/?device-1=samsung-galaxy-s20-5g&device-2=samsung-galaxy-s20%2B-5g&device-3=samsung-galaxy-s21-5g (last accessed June 17, 2021).

[. . .]

PLATFORM	OS	Android 10, upgradable to Android 11, One UI 3.0	Android 10, upgradable to Android 11, One UI 3.0	Android 10, upgradable to Android 11, One UI 3.0
	Chipset	Exynos 990 (7 nm+) - Global	Exynos 990 (7 nm+) - Global	Exynos 990 (7 nm+) - Global
		Qualcomm SM8250 Snapdragon 865 5G (7 nm+) - USA	Qualcomm SM8250 Snapdragon 865 5G (7 nm+) - USA	Qualcomm SM8250 Snapdragon 865 5G (7 nm+) - USA
	CPU	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55) - Global	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55) - Global	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55) - Global
		Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585) - USA	Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585) - USA	Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585) - USA

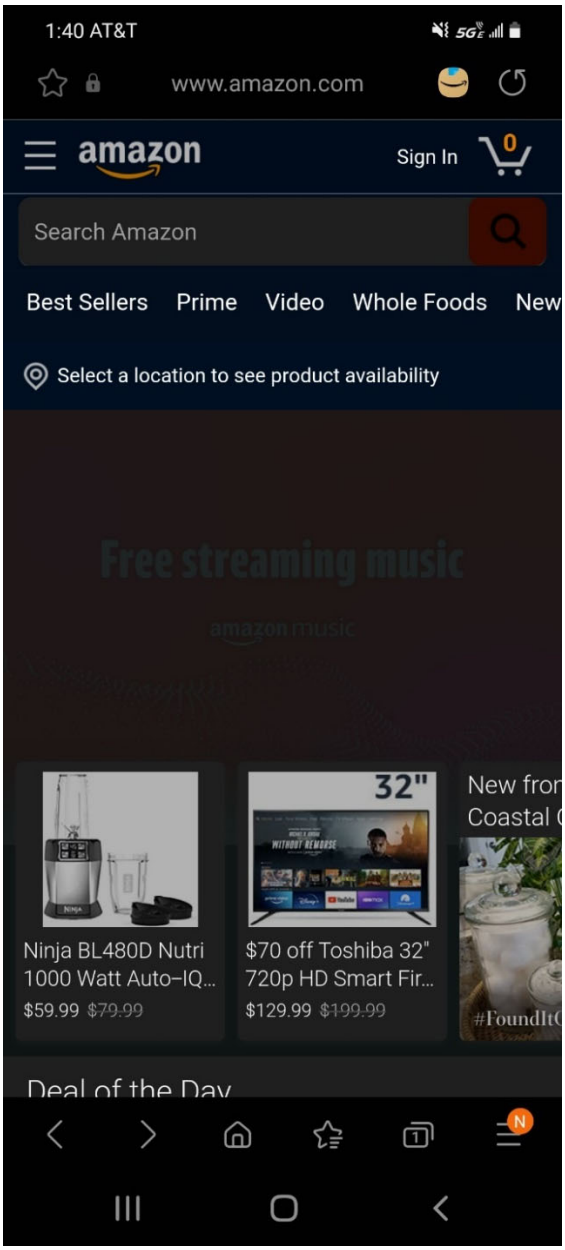
SAMSUNG GALAXY S20 COMPARISON, GSM ARENA, https://www.gsmarena.com/compare.php3?idPhone1=10081&idPhone2=10080&idPhone3=10040 (last accessed June 17, 2021).



PLATFORM	OS	Android 11, One UI 3.1
	Chipset	Exynos 2100 (5 nm) - International
		Qualcomm SM8350 Snapdragon 888 5G (5 nm) - USA/China
	CPU	Octa-core (1x2.9 GHz Cortex-X1 & 3x2.80 GHz Cortex-A78 & 4x2.2 GHz Cortex-A55) - International
		Octa-core (1x2.84 GHz Kryo 680 & 3x2.42 GHz Kryo 680 & 4x1.80 GHz Kryo 680) - USA/China

SAMSUNG GALAXY S21 5G, GSM ARENA, https://www.gsmarena.com/samsung_galaxy_s21_5g-10626.php (last accessed June 17, 2021) (Galaxy S21 Specifications).

52. The Samsung Accused Products comprise a first processor of a first device configured to: based at least in part on a request from a user to access an external resource, communicate with a second processor using a restricted interface, wherein the second processor is configured to access at least one record stored at least in part in a secure storage. This is supported by the exemplary evidence below.



Screenshot taken on a US-variant Samsung Galaxy S20 mobile phone (taken June 7, 2021).

Strengthening Hardware Security with Galaxy S20's Secure Processor, SAMSUNG NEWSROOM (May 15, 2020), https://news.samsung.com/global/strengthening-hardware-security-with-galaxy-s20s-secure-processor (last accessed June 17, 2021).

As our latest flagship device, the Galaxy S20 series features the premium technologies that Galaxy fans have come to know and expect. The most secure device Samsung has ever made, the Galaxy S20 is protected by Knox—the industry-leading mobile security platform that protects the device from the chip level through to the software level. The Galaxy S20 also features a new, secure processor which protects against hardware-based attacks.

Introducing the Samsung S20: Our Most Secure Device Yet, SAMSUNG KNOX BLOG (Mar. 6, 2020), https://www.samsungknox.com/en/blog/introducing-the-samsung-galaxy-s20-our-most-secure-device-yet (last accessed June 17, 2021).

Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices

Korea on February 26, 2020 Audio Share

Samsung's new Secure Element solution features secure key storage with CC EAL 5+ certification and dedicated security software for enhanced data protection

Samsung Electronics, a world leader in advanced semiconductor technology, today introduced a Common Criteria Evaluation Assurance Level (CC EAL) 5+ certified Secure Element (SE) turnkey solution for mobile devices. The new SE offers a strong security solution, consisting of a security chip (S3K250AF) and optimized software, that fully guards private data on an isolated data storage.

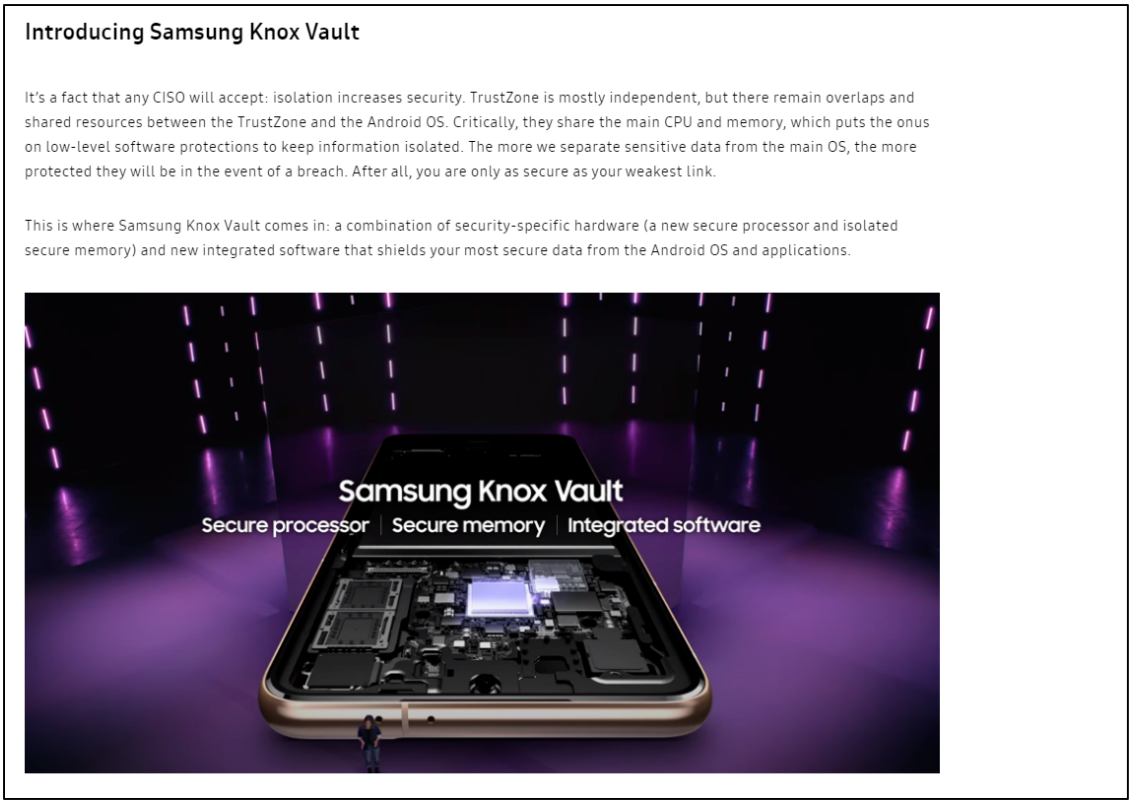
Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices, SAMSUNG NEWSROOM (Feb. 26, 2020), https://news.samsung.com/global/samsung-introduces-best-in-class-data-security-chip-solution-for-mobile-devices (last accessed June 17, 2021).

Security

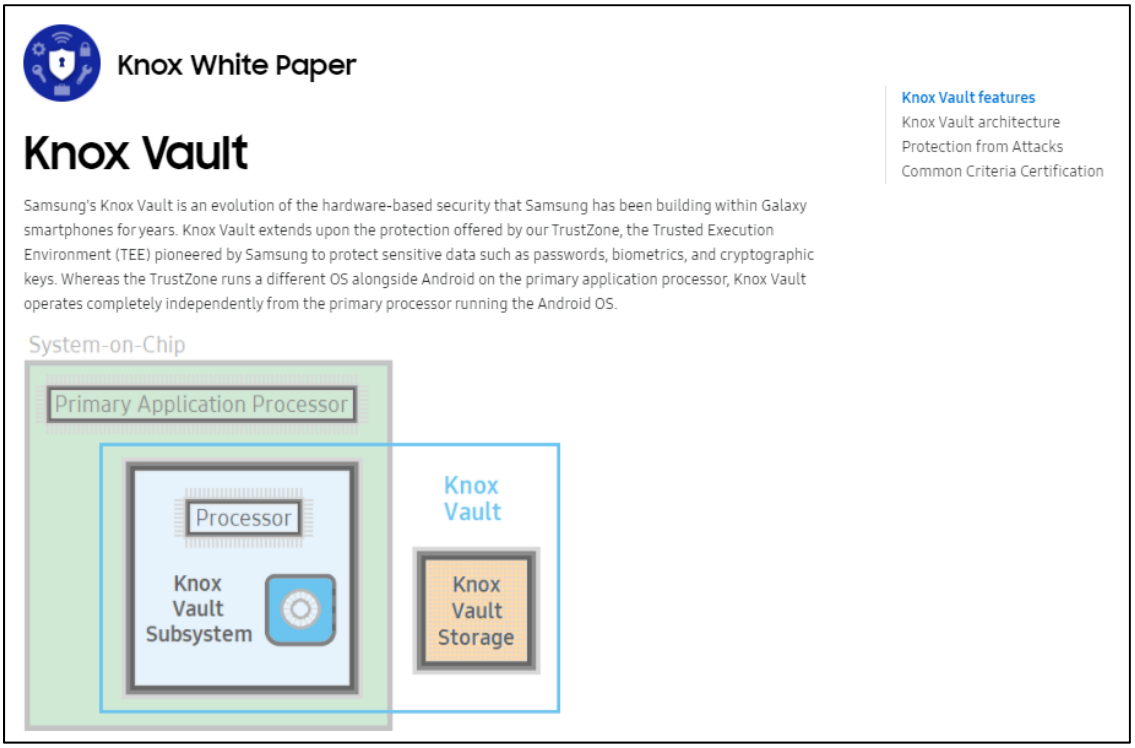
Of course, when it comes to security, we always have your back. As usual, we built the S21 on the Samsung Knox defense-grade security platform, which defends your device against hackers, malware and other threats. It's your secure foundation for everything you want to protect on your phone, including biometrics, mobile payments and health data.

To take security to the next level, the S21 introduces Knox Vault, a chipset-level security platform. By adding tamper-resistant secure memory to our secure processor, Knox Vault adds a further layer of protection to guard against physical, fault and side-channel attacks.

Hamshy Raveendran, *Introducing the Galaxy S21: Supporting Today's Hybrid Workplace*, SAMSUNG INSIGHTS (Jan. 14, 2021), https://insights.samsung.com/2021/01/14/introducing-the-galaxy-s21-supporting-todays-hybrid-workplace/ (last accessed June 17, 2021).



David Thomson, *Understanding Samsung Knox Vault: Protecting the data that matters most*, SAMSUNG NEWSROOM U.S. (Mar. 3, 2021), https://news.samsung.com/us/understanding-samsung-knox-vault-protecting-data-matters-most/.



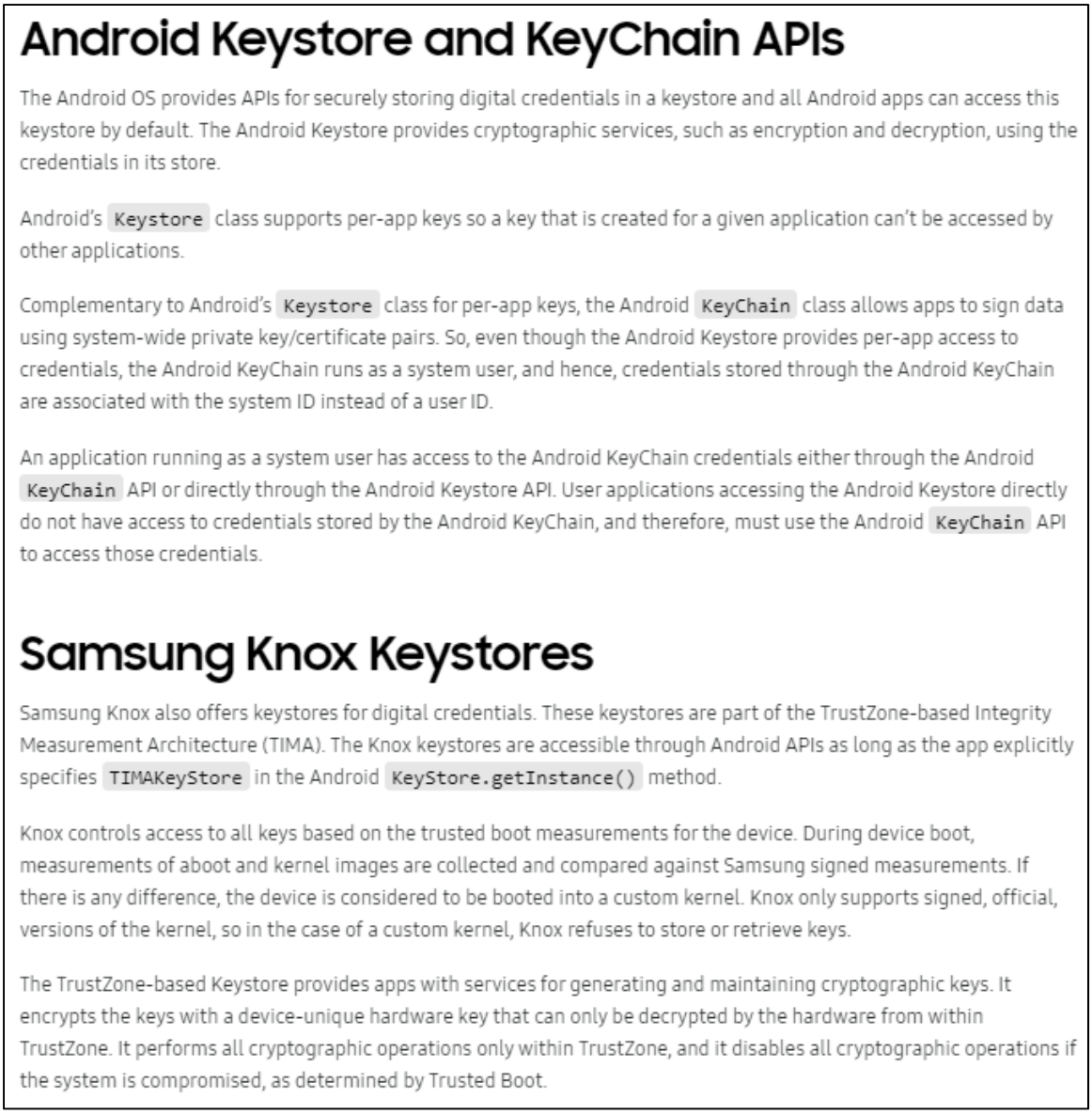
[. . .]

> As a core component of the Knox security platform, Knox Vault is an isolated, tamper-proof, secure subsystem with its own processor and memory, as well as an interface to dedicated, non-volatile secure storage. Knox Vault can:
>
> - Store sensitive data such as hardware-backed Android Keystore keys, the Samsung Attestation Key (SAK), biometric data, and blockchain credentials.
> - Run security-critical code that authenticates users with increasing timeouts between failures and controls access to keys depending on authentication.

KNOX WHITE PAPER, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

> **9. Defense-grade Knox security**
>
> Samsung has always been at the forefront of mobile device security. The Galaxy S21 is no different, thanks to Samsung Knox, a defense-grade solution for keeping your work and your business protected from the chip up. Knox defends your S21 from intrusions, malware and other malicious threats. The S21 devices also introduce Knox Vault, which combines tamper-resistant secure memory with our secure processor for an additional layer of protection. This advanced security architecture keeps your data — including your Blockchain private key, Samsung Pay credentials and more — out of unauthorized hands.

Michael Archambault, *10 Reasons to Upgrade to the Galaxy S21*, SAMSUNG INSIGHTS (Jan. 14, 2021), https://insights.samsung.com/2021/01/14/10-reasons-to-upgrade-to-the-galaxy-s21/.



Android Keystore and KeyChain APIs

The Android OS provides APIs for securely storing digital credentials in a keystore and all Android apps can access this keystore by default. The Android Keystore provides cryptographic services, such as encryption and decryption, using the credentials in its store.

Android's `Keystore` class supports per-app keys so a key that is created for a given application can't be accessed by other applications.

Complementary to Android's `Keystore` class for per-app keys, the Android `KeyChain` class allows apps to sign data using system-wide private key/certificate pairs. So, even though the Android Keystore provides per-app access to credentials, the Android KeyChain runs as a system user, and hence, credentials stored through the Android KeyChain are associated with the system ID instead of a user ID.

An application running as a system user has access to the Android KeyChain credentials either through the Android `KeyChain` API or directly through the Android Keystore API. User applications accessing the Android Keystore directly do not have access to credentials stored by the Android KeyChain, and therefore, must use the Android `KeyChain` API to access those credentials.

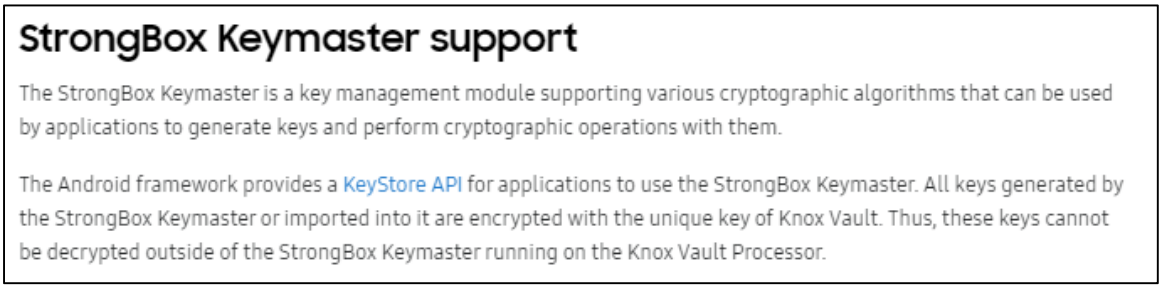
Samsung Knox Keystores

Samsung Knox also offers keystores for digital credentials. These keystores are part of the TrustZone-based Integrity Measurement Architecture (TIMA). The Knox keystores are accessible through Android APIs as long as the app explicitly specifies `TIMAKeyStore` in the Android `KeyStore.getInstance()` method.

Knox controls access to all keys based on the trusted boot measurements for the device. During device boot, measurements of aboot and kernel images are collected and compared against Samsung signed measurements. If there is any difference, the device is considered to be booted into a custom kernel. Knox only supports signed, official, versions of the kernel, so in the case of a custom kernel, Knox refuses to store or retrieve keys.

The TrustZone-based Keystore provides apps with services for generating and maintaining cryptographic keys. It encrypts the keys with a device-unique hardware key that can only be decrypted by the hardware from within TrustZone. It performs all cryptographic operations only within TrustZone, and it disables all cryptographic operations if the system is compromised, as determined by Trusted Boot.

TIMA Keystore, KNOX DEVELOPER DOCUMENTATION: KNOX SDK, https://docs.samsungknox.com/dev/knox-sdk/about-keystores.htm (last accessed June 17, 2021).



StrongBox Keymaster support

The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.

The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

Knox White Paper, KNOX DOCUMENTATION, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

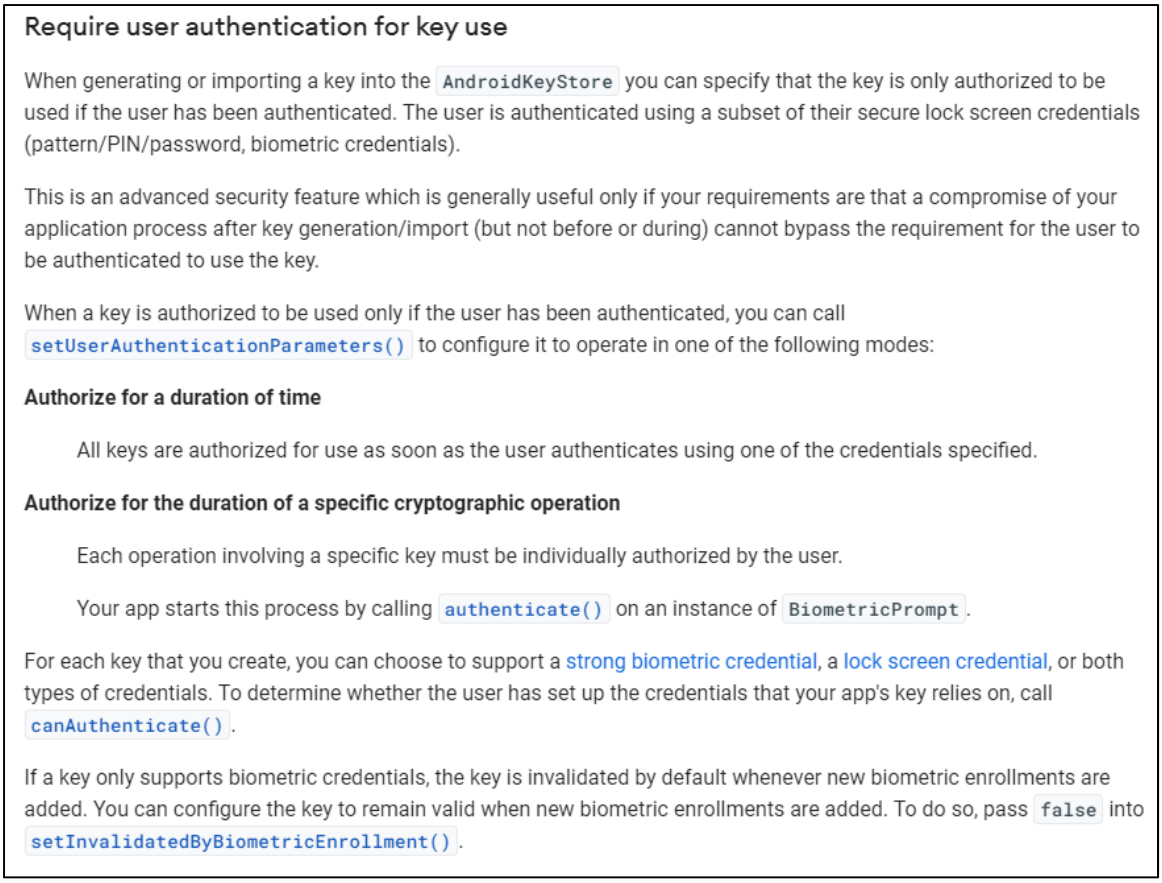
53. The Samsung Accused Products comprise a first processor of a first device configured to: based at least in part on a request from a user to access an external resource, communicate with a second processor using a restricted interface, wherein the second processor is configured to access at least one record stored at least in part in a secure storage, wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising at least one of a password, a cookie, or a cryptographic key. This is supported by the exemplary evidence below.

> In the Android OS, fingerprint biometrics are required to be stored in the Trusted Execution Environment (TEE), where the information is encrypted and kept in a separate part of the smartphone, completely inaccessible to the regular OS. It can't even be exported. Android can ask the TEE to verify a user's identity using biometrics, but it can't extract the biometric information. In other words, when the user stores their biometric information, such as a fingerprint, they're not sharing that information outside of their own smartphone or tablet; they're just establishing a way to identify themselves to their device.

[. . .]

> Samsung Pass is an example of a password management service that's based on the FIDO specifications. Samsung Pass enables strong authentication across different apps using biometrics combined with a cloud-based service, provided by Samsung. Smartphone users can lock up multiple sets of authentication credentials — from both public and private enterprise services — and protect them with their fingerprint. Samsung Pass simplifies the user experience while using highly secure authentication systems based on digital certificates, so end users can keep their strong authentication credentials locked up with biometrics, reduce their use of insecure passwords and speed up their app authentication.

Joel Snyder, *Using Biometrics for Authentication in Android*, SAMSUNG INSIGHTS (Apr. 21, 2021), https://insights.samsung.com/2021/04/21/using-biometrics-for-authentication-in-android-2/ (last accessed June 17, 2021).



Require user authentication for key use

When generating or importing a key into the `AndroidKeyStore` you can specify that the key is only authorized to be used if the user has been authenticated. The user is authenticated using a subset of their secure lock screen credentials (pattern/PIN/password, biometric credentials).

This is an advanced security feature which is generally useful only if your requirements are that a compromise of your application process after key generation/import (but not before or during) cannot bypass the requirement for the user to be authenticated to use the key.

When a key is authorized to be used only if the user has been authenticated, you can call `setUserAuthenticationParameters()` to configure it to operate in one of the following modes:

Authorize for a duration of time

All keys are authorized for use as soon as the user authenticates using one of the credentials specified.

Authorize for the duration of a specific cryptographic operation

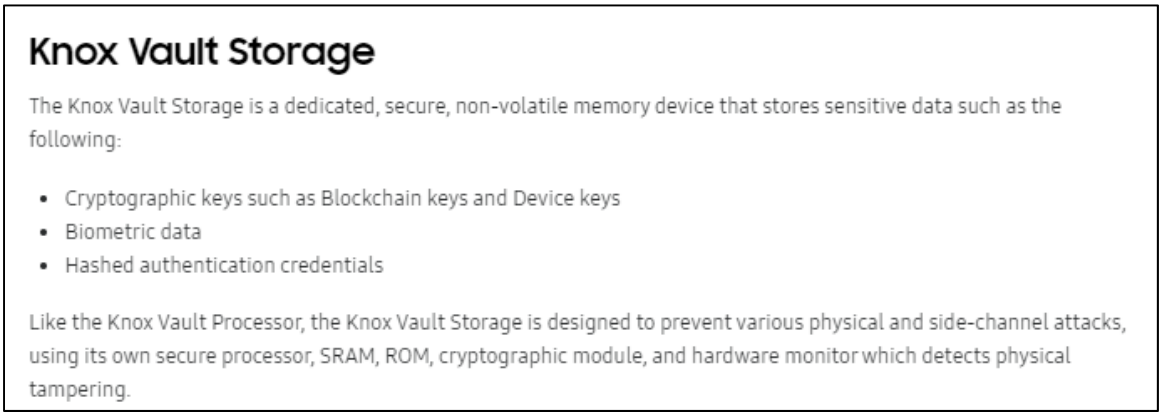
Each operation involving a specific key must be individually authorized by the user.

Your app starts this process by calling `authenticate()` on an instance of `BiometricPrompt`.

For each key that you create, you can choose to support a strong biometric credential, a lock screen credential, or both types of credentials. To determine whether the user has set up the credentials that your app's key relies on, call `canAuthenticate()`.

If a key only supports biometric credentials, the key is invalidated by default whenever new biometric enrollments are added. You can configure the key to remain valid when new biometric enrollments are added. To do so, pass `false` into `setInvalidatedByBiometricEnrollment()`.

Android Keystore System, ANDROID DEVELOPER DOCUMENTATION, https://developer.android.com/training/articles/keystore (last accessed June 17, 2021).



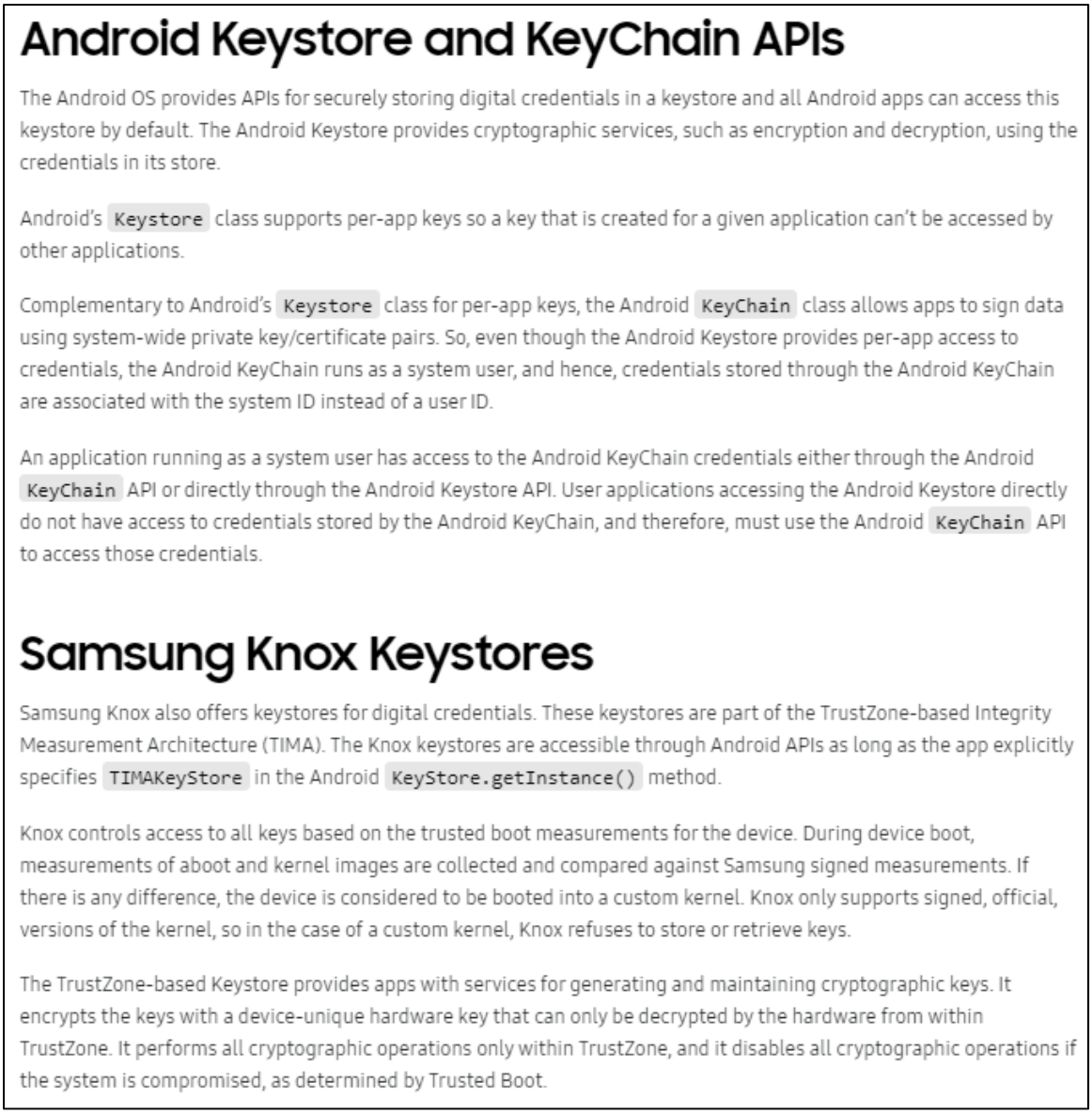
Knox Vault Storage

The Knox Vault Storage is a dedicated, secure, non-volatile memory device that stores sensitive data such as the following:

- Cryptographic keys such as Blockchain keys and Device keys
- Biometric data
- Hashed authentication credentials

Like the Knox Vault Processor, the Knox Vault Storage is designed to prevent various physical and side-channel attacks, using its own secure processor, SRAM, ROM, cryptographic module, and hardware monitor which detects physical tampering.

Knox White Paper, KNOX DOCUMENTATION, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).



Android Keystore and KeyChain APIs

The Android OS provides APIs for securely storing digital credentials in a keystore and all Android apps can access this keystore by default. The Android Keystore provides cryptographic services, such as encryption and decryption, using the credentials in its store.

Android's `Keystore` class supports per-app keys so a key that is created for a given application can't be accessed by other applications.

Complementary to Android's `Keystore` class for per-app keys, the Android `KeyChain` class allows apps to sign data using system-wide private key/certificate pairs. So, even though the Android Keystore provides per-app access to credentials, the Android KeyChain runs as a system user, and hence, credentials stored through the Android KeyChain are associated with the system ID instead of a user ID.

An application running as a system user has access to the Android KeyChain credentials either through the Android `KeyChain` API or directly through the Android Keystore API. User applications accessing the Android Keystore directly do not have access to credentials stored by the Android KeyChain, and therefore, must use the Android `KeyChain` API to access those credentials.

Samsung Knox Keystores

Samsung Knox also offers keystores for digital credentials. These keystores are part of the TrustZone-based Integrity Measurement Architecture (TIMA). The Knox keystores are accessible through Android APIs as long as the app explicitly specifies `TIMAKeyStore` in the Android `KeyStore.getInstance()` method.

Knox controls access to all keys based on the trusted boot measurements for the device. During device boot, measurements of aboot and kernel images are collected and compared against Samsung signed measurements. If there is any difference, the device is considered to be booted into a custom kernel. Knox only supports signed, official, versions of the kernel, so in the case of a custom kernel, Knox refuses to store or retrieve keys.

The TrustZone-based Keystore provides apps with services for generating and maintaining cryptographic keys. It encrypts the keys with a device-unique hardware key that can only be decrypted by the hardware from within TrustZone. It performs all cryptographic operations only within TrustZone, and it disables all cryptographic operations if the system is compromised, as determined by Trusted Boot.

TIMA Keystore, KNOX DEVELOPER DOCUMENTATION: KNOX SDK, https://docs.samsungknox.com/dev/knox-sdk/about-keystores.htm (last accessed June 17, 2021).

Samsung's new Secure Element solution features secure key storage with CC EAL 5+ certification and dedicated security software for enhanced data protection

Samsung Electronics, a world leader in advanced semiconductor technology, today introduced a Common Criteria Evaluation Assurance Level (CC EAL) 5+ certified Secure Element (SE) turnkey solution for mobile devices. The new SE offers a strong security solution, consisting of a security chip (S3K250AF) and optimized software, that fully guards private data on an isolated data storage.

[. . .]

> From checking emails and making online payments to replacing house keys and airplane tickets, smart devices continue to offer more applications that enforce stronger security requirements. Samsung's new turnkey solution is a dedicated tamper-resistant strongbox that securely stores users' confidential and cryptographic data such as pin numbers, passwords and even crypto-currency credentials separate from the typical mobile memory such as embedded Universal Flash Storage (eUFS).

Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices, SAMSUNG NEWSROOM (Feb. 26, 2020), https://news.samsung.com/global/samsung-introduces-best-in-class-data-security-chip-solution-for-mobile-devices (last accessed June 17, 2021).

> ## Weaver
>
> Weaver is used for secure password authentication to Android. Running on the Knox Vault Processor, Weaver's data and secrets (passwords) are stored encrypted in the secure Knox Vault Storage. When Weaver receives the secret data to be stored, it also receives a key, and this key must be provided to read the secret data again from Weaver.
>
> To prevent brute-force attempts to extract secrets, Weaver uses a binary exponential back-off algorithm. When attempting to read a secret, if the proper key is not provided, Weaver declines read operations for a time period decided by the back-off algorithm. A non-bypassable secure timer is used to track these time periods.
>
> ## Credential storage
>
> This feature stores data encrypted by the Knox Vault Processor in the Knox Vault Storage, using a secure channel to protect data transfered between the Knox Vault Processor and the Knox Vault Storage.
>
> The following data is stored in the Knox Vault Storage:
>
> - Cryptographic keys to protect biometric data
> - Blockchain keystore credentials
> - Samsung Attestation Key (SAK)
>
> All data in Credential Storage is encrypted using a Knox Vault-unique key. This prevents the data from being decrypted in other devices.

[. . .]

> ## StrongBox Keymaster support
>
> The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.
>
> The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

Knox White Paper, KNOX DOCUMENTATION, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

54. The Samsung Accused Products comprise a first processor of a first device configured to: in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input

corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, and wherein the biometric input is received subsequent to presenting of a prompt. This is supported by the exemplary evidence below.

SECURITY TIPS

Using biometrics for authentication in Android

Published Apr 21, 2021 By: Joel Snyder

To unlock their mobile devices more simply, users are now favoring biometric authentication, such as fingerprint sensors, which also reduce the cognitive burden of remembering multiple long passwords.

Proper use of biometrics increases security, too. Passwords are easy to steal; faking biometrics is much more difficult. The technology is ideal for providing role-based access controls — and a high level of trust for business users.

Here's a detailed look at how biometrics work, how data encryption fits in and what business leaders should look for to maintain strong security while delivering the convenience users want:

How biometrics work

Unlike passwords or PINs, biometrics aren't saved in the network or passed around between devices and servers. Instead, biometrics protect other authentication information — usually a digital certificate or private key — and it's this protected information that is actually used to verify the user.

[. . .]

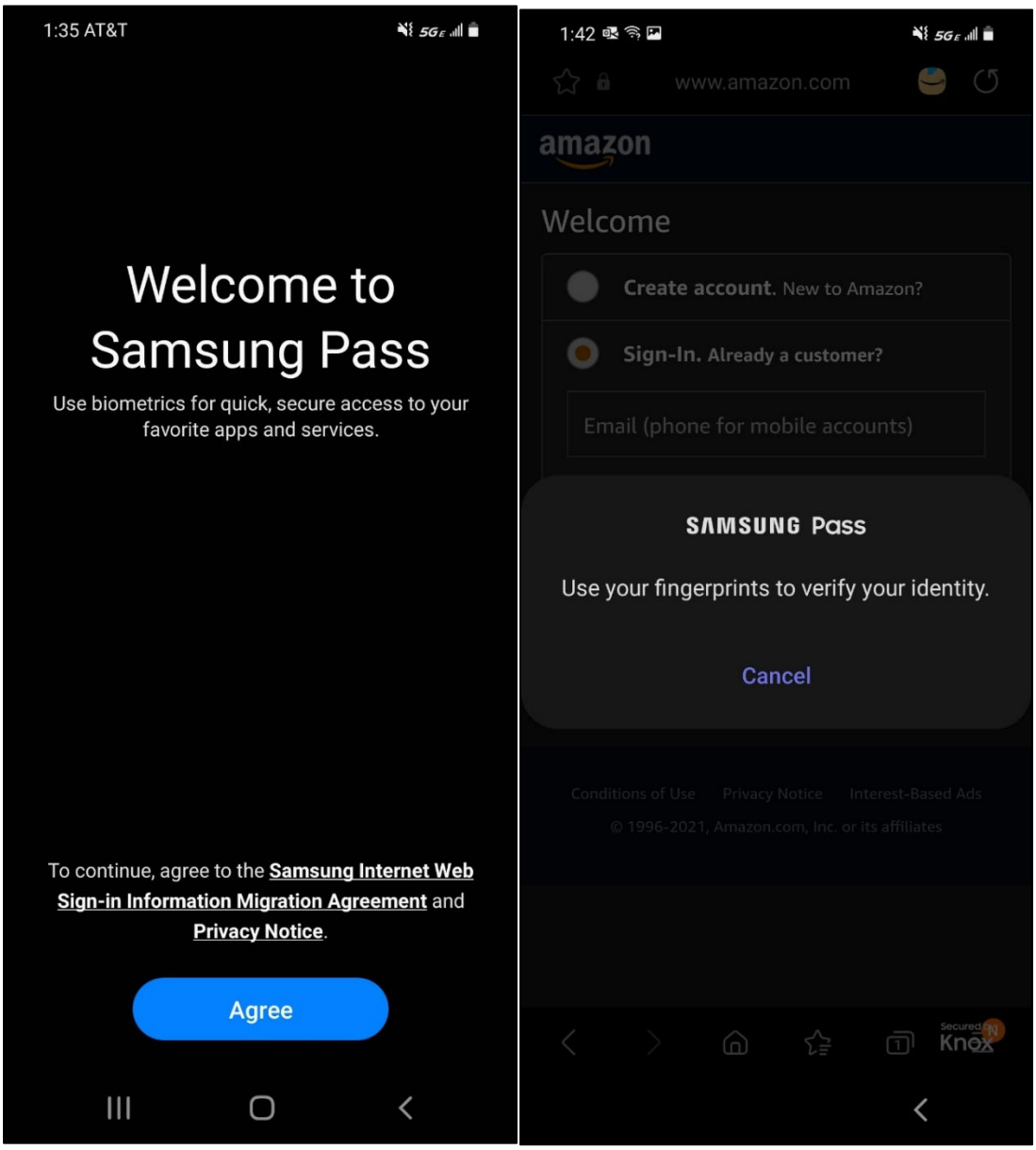
In the Android OS, fingerprint biometrics are required to be stored in the Trusted Execution Environment (TEE), where the information is encrypted and kept in a separate part of the smartphone, completely inaccessible to the regular OS. It can't even be exported. Android can ask the TEE to verify a user's identity using biometrics, but it can't extract the biometric information. In other words, when the user stores their biometric information, such as a fingerprint, they're not sharing that information outside of their own smartphone or tablet; they're just establishing a way to identify themselves to their device.

Joel Snyder, *Using Biometrics for Authentication in Android,* SAMSUNG INSIGHTS (Apr. 21, 2021), https://insights.samsung.com/2021/04/21/using-biometrics-for-authentication-in-android-2/ (last accessed June 17, 2021).

Set up and use Samsung Pass on your Galaxy phone

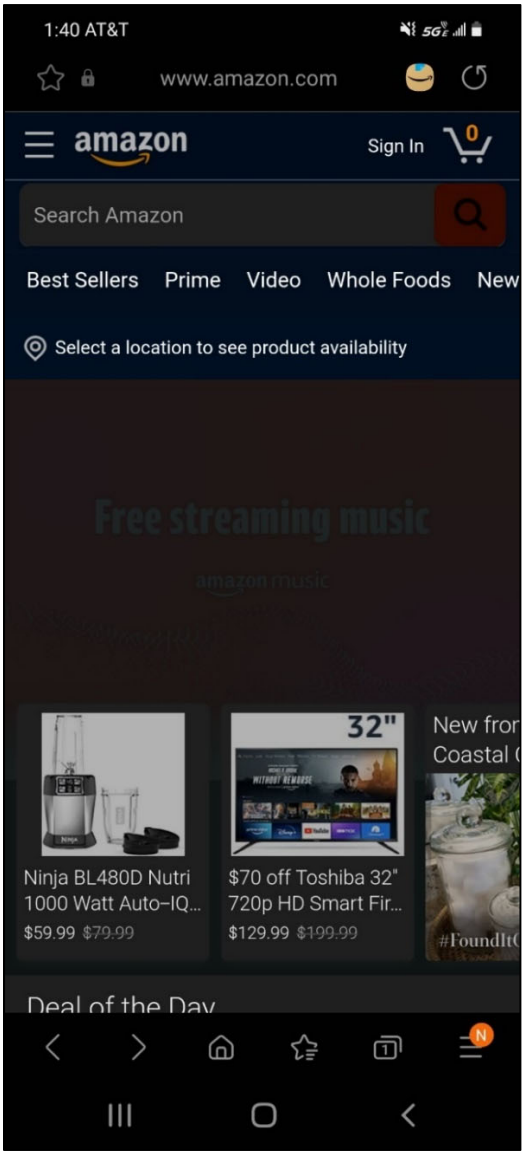
Finally, no more memorizing all those different IDs and passwords for websites and apps. Samsung Pass uses biometric data like your fingerprints or irises to authenticate your identity, keeping your accounts safe and secure.

SET UP AND USE SAMSUNG PASS ON YOUR GALAXY PHONE, https://www.samsung.com/us/support/answer/ANS00062705/ (last accessed June 17, 2021).



Screenshots taken on a US-variant Samsung Galaxy S20 mobile phone (taken June 7, 2021).

55. The Samsung Accused Products comprise a first processor of a first device configured to: establish a connection with the external resource. This is supported by the exemplary evidence below.



Screenshot taken on a US-variant Samsung Galaxy S20 mobile phone (taken June 7, 2021) (As an example, the Accused Products receive a request associated with a user, such as a click on the screen, to access an external resource such as Amazon's webpage.).

56. The Samsung Accused Products comprise a first processor of a first device configured to: facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output. This is supported by the exemplary evidence below.

SECURITY TIPS

Using biometrics for authentication in Android

Published Apr 21, 2021 By: Joel Snyder

To unlock their mobile devices more simply, users are now favoring biometric authentication, such as fingerprint sensors, which also reduce the cognitive burden of remembering multiple long passwords.

Proper use of biometrics increases security, too. Passwords are easy to steal; faking biometrics is much more difficult. The technology is ideal for providing role-based access controls — and a high level of trust for business users.

Here's a detailed look at how biometrics work, how data encryption fits in and what business leaders should look for to maintain strong security while delivering the convenience users want:

How biometrics work

Unlike passwords or PINs, biometrics aren't saved in the network or passed around between devices and servers. Instead, biometrics protect other authentication information — usually a digital certificate or private key — and it's this protected information that is actually used to verify the user.

[. . .]

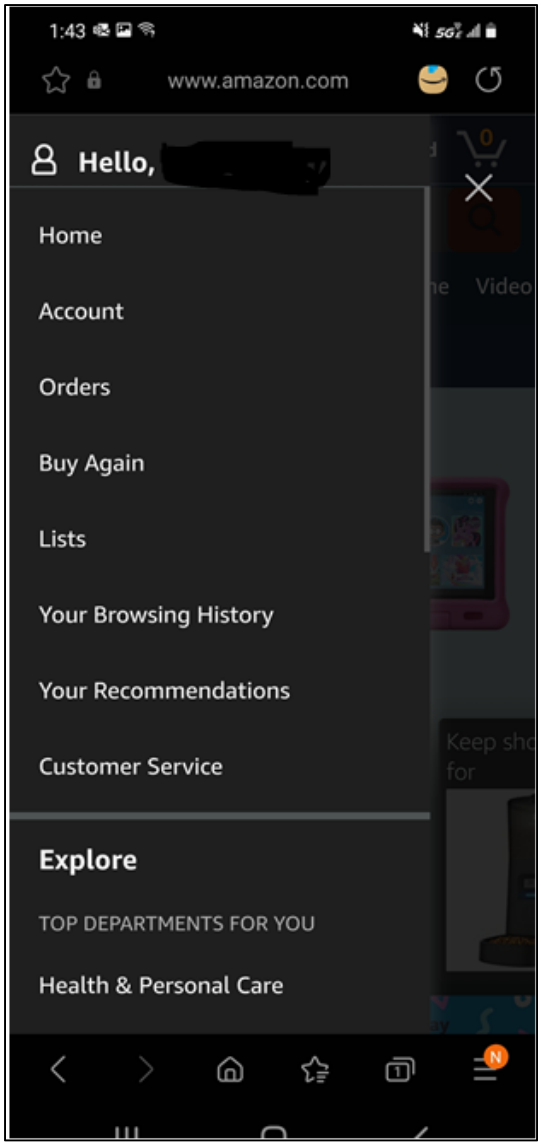
In the Android OS, fingerprint biometrics are required to be stored in the Trusted Execution Environment (TEE), where the information is encrypted and kept in a separate part of the smartphone, completely inaccessible to the regular OS. It can't even be exported. Android can ask the TEE to verify a user's identity using biometrics, but it can't extract the biometric information. In other words, when the user stores their biometric information, such as a fingerprint, they're not sharing that information outside of their own smartphone or tablet; they're just establishing a way to identify themselves to their device.

Joel Snyder, *Using Biometrics for Authentication in Android*, SAMSUNG INSIGHTS (Apr. 21, 2021), https://insights.samsung.com/2021/04/21/using-biometrics-for-authentication-in-android-2/ (last accessed June 17, 2021).

Set up and use Samsung Pass on your Galaxy phone

Finally, no more memorizing all those different IDs and passwords for websites and apps. Samsung Pass uses biometric data like your fingerprints or irises to authenticate your identity, keeping your accounts safe and secure.

SET UP AND USE SAMSUNG PASS ON YOUR GALAXY PHONE, https://www.samsung.com/us/support/answer/ANS00062705/ (last accessed June 17, 2021).



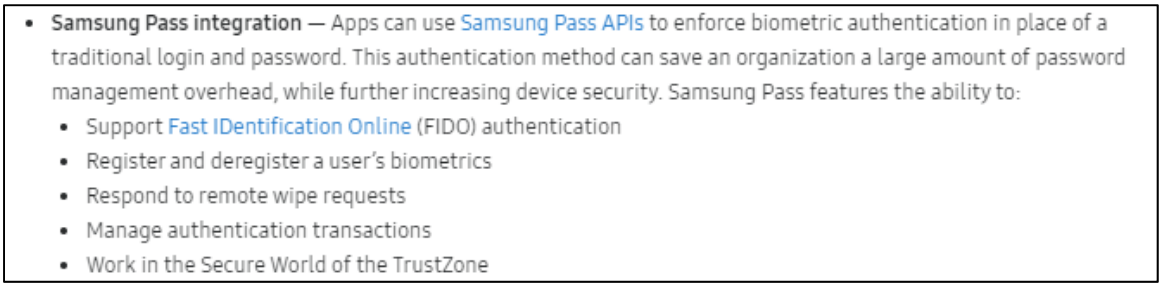
Screenshot taken on a US-variant Samsung Galaxy S20 mobile phone (taken June 7, 2021) (account information redacted).

57. The Samsung Accused Products comprise a first processor of a first device configured to: facilitate wiping of at least a portion of the at least one record. This is supported by the exemplary evidence below.

What is the Find My Mobile service?

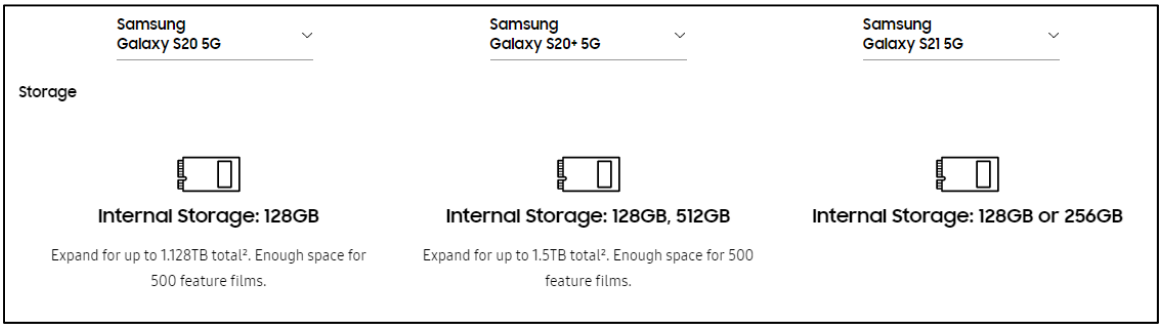
Samsung's Find My Mobile is a free service that is accessed via your Samsung account and allows you to locate, remotely backup and wipe data on a registered Galaxy mobile device. It can be accessed at findmymobile.samsung.com.

Shane, Schick, *How to use Samsung Find My Mobile*, SAMSUNG INSIGHTS (Sep. 30, 2020), https://insights.samsung.com/2020/09/30/how-to-use-samsung-find-my-mobile/ (last accessed June 17, 2021).

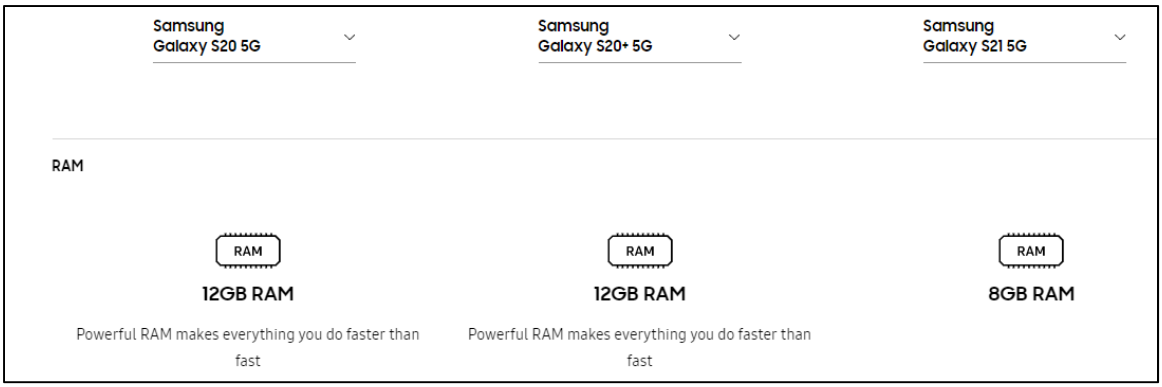


BIOMETRIC AUTHENTICATION, KNOX WHITE PAPER, https://docs.samsungknox.com/admin/whitepaper/kpe/biometric-authentication.htm (last accessed June 15, 2021).

58. The Samsung Accused Products comprise a memory coupled to the first processor and configured to provide the first processor with instructions. This is supported by the exemplary evidence below.



[. . .]



HOW THE SAMSUNG S20 FE 5G COMPARES, https://www.samsung.com/us/mobile/galaxy-s20-5g/compare/?device-1=samsung-galaxy-s20-5g&device-2=samsung-galaxy-s20%2B-5g&device-3=samsung-galaxy-s21-5g (last accessed June 17, 2021).

59. Samsung also indirectly infringes claims of the ’696 Patent, as provided in 35 U.S.C. § 271(b), by inducing infringement by others, such as Samsung’s customers and end users, in this District and elsewhere in the United States. For example, Samsung’s customers and end users directly infringe through their use of the inventions claimed in the ’696 Patent. Samsung induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products and related services, and providing instructions, documentation, online technical support, marketing, product manuals, advertisements, and other information to customers and end users suggesting they use the Accused Products and related services in an infringing manner. As a result of Samsung’s inducement, Samsung’s customers and end users use the Accused Products and related services in the way Samsung intends and directly infringe the ’696 Patent.

COUNT II: PATENT INFRINGEMENT OF THE ’512 PATENT

60. RightQuestion incorporates by reference the preceding paragraphs as if fully stated herein.

61. Samsung has been and is now directly infringing and/or indirectly infringing the ’512 Patent by way of inducement and/or contributory infringement, literally and/or under the Doctrine of Equivalents, in violation of 35 U.S.C. § 271, including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least ’512 accused products. Samsung derives revenue from the activities relating to the ’512 accused products. As explained below, these products are covered by one or more claims of the ’512 Patent, including but not limited to claims 1-4, 6, 7-15, and 17-21.

62. For example, claim 1 of the ’512 patent is reproduced below:

1. A system, comprising:

a first processor of a first device, wherein the first processor is configured to:

based at least in part on a request associated with a user to access an external resource, establish a secure connection with the external resource; and

communicate with a second processor using a restricted interface, wherein the second processor is configured to:

receive a biometric input from a sensor, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature; and

access a record stored in a secure storage, wherein the record is associated at least with the external resource;

retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;

perform a cryptographic operation;

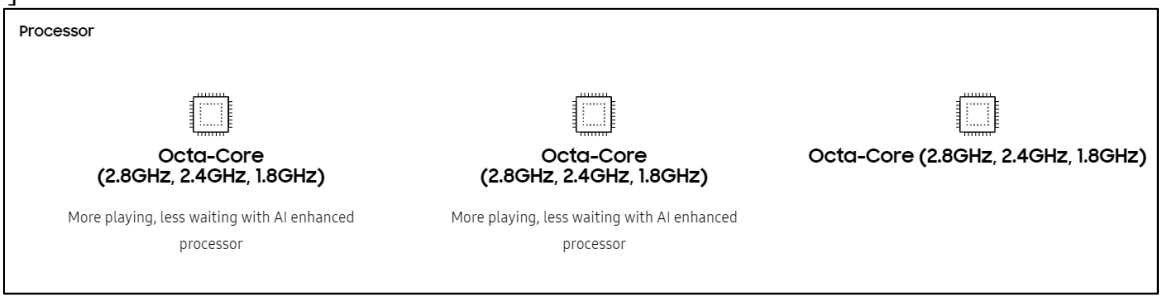
in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output; and

perform a secure backup of the record to a storage service, wherein a second device associated with the user is registered with the storage service, and wherein the record is downloaded from the storage service by the second device; and

a memory coupled to the first processor and configured to provide the first processor with instructions.

63. As a non-limiting example, the Samsung Accused Products are systems comprising a first processor of a first device, wherein the first processor is configured to perform the limitations below. This is supported by the exemplary evidence below.

[. . .]

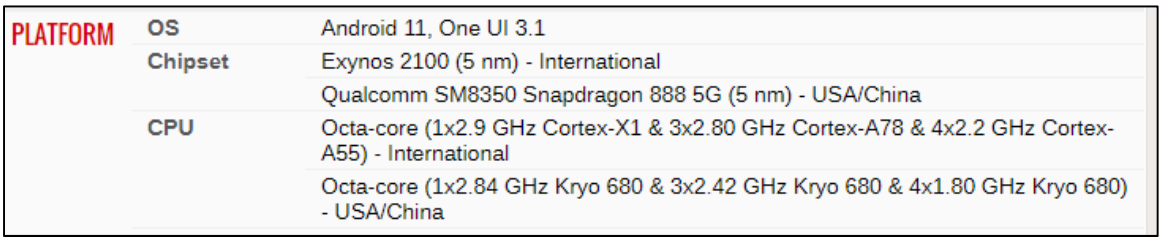


HOW THE SAMSUNG S20 FE 5G COMPARES, https://www.samsung.com/us/mobile/galaxy-s20-5g/compare/?device-1=samsung-galaxy-s20-5g&device-2=samsung-galaxy-s20%2B-5g&device-3=samsung-galaxy-s21-5g (last accessed June 17, 2021).

[. . .]

PLATFORM	OS	Android 10, upgradable to Android 11, One UI 3.0	Android 10, upgradable to Android 11, One UI 3.0	Android 10, upgradable to Android 11, One UI 3.0
	Chipset	Exynos 990 (7 nm+) - Global	Exynos 990 (7 nm+) - Global	Exynos 990 (7 nm+) - Global
		Qualcomm SM8250 Snapdragon 865 5G (7 nm+) - USA	Qualcomm SM8250 Snapdragon 865 5G (7 nm+) - USA	Qualcomm SM8250 Snapdragon 865 5G (7 nm+) - USA
	CPU	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55) - Global	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55) - Global	Octa-core (2x2.73 GHz Mongoose M5 & 2x2.50 GHz Cortex-A76 & 4x2.0 GHz Cortex-A55) - Global
		Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585) - USA	Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585) - USA	Octa-core (1x2.84 GHz Kryo 585 & 3x2.42 GHz Kryo 585 & 4x1.8 GHz Kryo 585) - USA

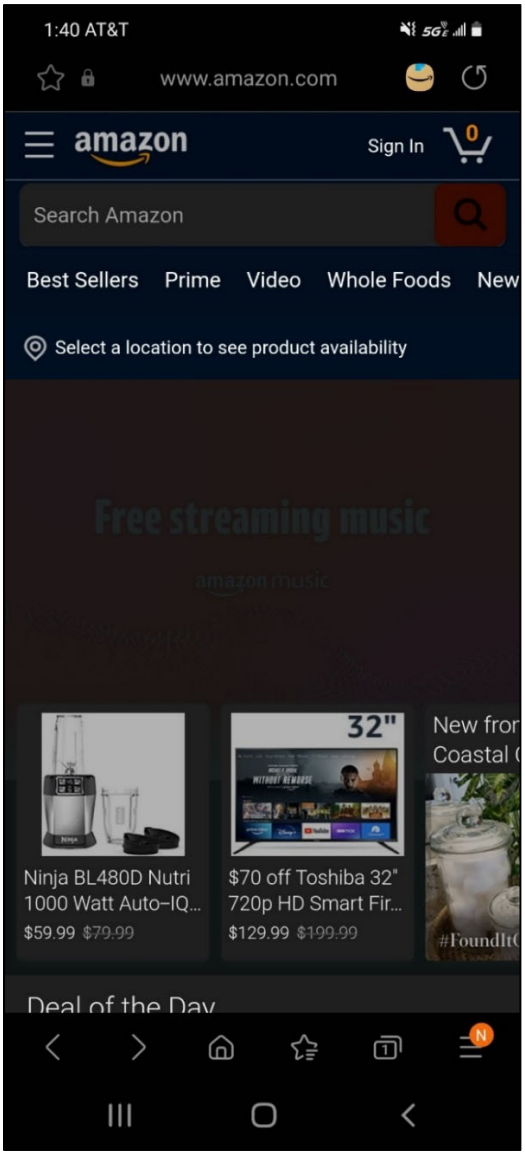
Samsung Galaxy S20 Comparison, GSM ARENA, https://www.gsmarena.com/compare.php3?idPhone1=10081&idPhone2=10080&idPhone3=10040 (last accessed June 17, 2021).



PLATFORM	OS	Android 11, One UI 3.1
	Chipset	Exynos 2100 (5 nm) - International
		Qualcomm SM8350 Snapdragon 888 5G (5 nm) - USA/China
	CPU	Octa-core (1x2.9 GHz Cortex-X1 & 3x2.80 GHz Cortex-A78 & 4x2.2 GHz Cortex-A55) - International
		Octa-core (1x2.84 GHz Kryo 680 & 3x2.42 GHz Kryo 680 & 4x1.80 GHz Kryo 680) - USA/China

Samsung Galaxy S21 5G, GSM ARENA, https://www.gsmarena.com/samsung_galaxy_s21_5g-10626.php (last accessed June 17, 2021) (Galaxy S21 Specifications).

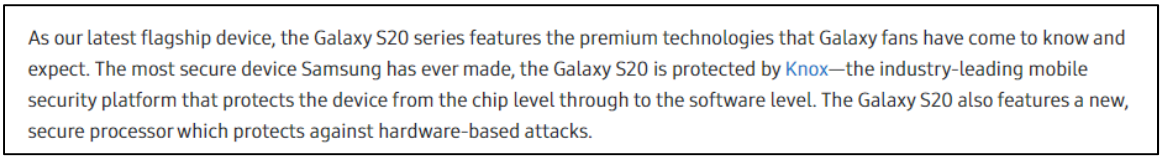
64. The Samsung Accused Products comprise a first processor of a first device configured to: based at least in part on a request associated with a user to access an external resource, establish a secure connection with the external resource. This is supported by the exemplary evidence below.



Screenshot taken on a US-variant Samsung Galaxy S20 mobile phone (taken June 7, 2021) (As an example, the Accused Products receive a request associated with a user, such as a click on the screen, to access an external resource such as Amazon's webpage. A secure connection (e.g., as indicated by the padlock symbol in the address bar of the browser) is established with the external resource.).

65. The Samsung Accused Products comprise a first processor of a first device configured to: communicate with a second processor using a restricted interface, wherein the second processor is configured to perform the limitations below. This is supported by the exemplary evidence below.

Strengthening Hardware Security with Galaxy S20's Secure Processor, SAMSUNG NEWSROOM (May 15, 2020), https://news.samsung.com/global/strengthening-hardware-security-with-galaxy-s20s-secure-processor (last accessed June 17, 2021).



Introducing the Samsung S20: Our Most Secure Device Yet, SAMSUNG KNOX BLOG (Mar. 6, 2020), https://www.samsungknox.com/en/blog/introducing-the-samsung-galaxy-s20-our-most-secure-device-yet (last accessed June 17, 2021).

Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices, SAMSUNG NEWSROOM (Feb. 26, 2020), https://news.samsung.com/global/samsung-introduces-best-in-class-data-security-chip-solution-for-mobile-devices (last accessed June 17, 2021).

Security

Of course, when it comes to security, we always have your back. As usual, we built the S21 on the Samsung Knox defense-grade security platform, which defends your device against hackers, malware and other threats. It's your secure foundation for everything you want to protect on your phone, including biometrics, mobile payments and health data.

To take security to the next level, the S21 introduces Knox Vault, a chipset-level security platform. By adding tamper-resistant secure memory to our secure processor, Knox Vault adds a further layer of protection to guard against physical, fault and side-channel attacks.

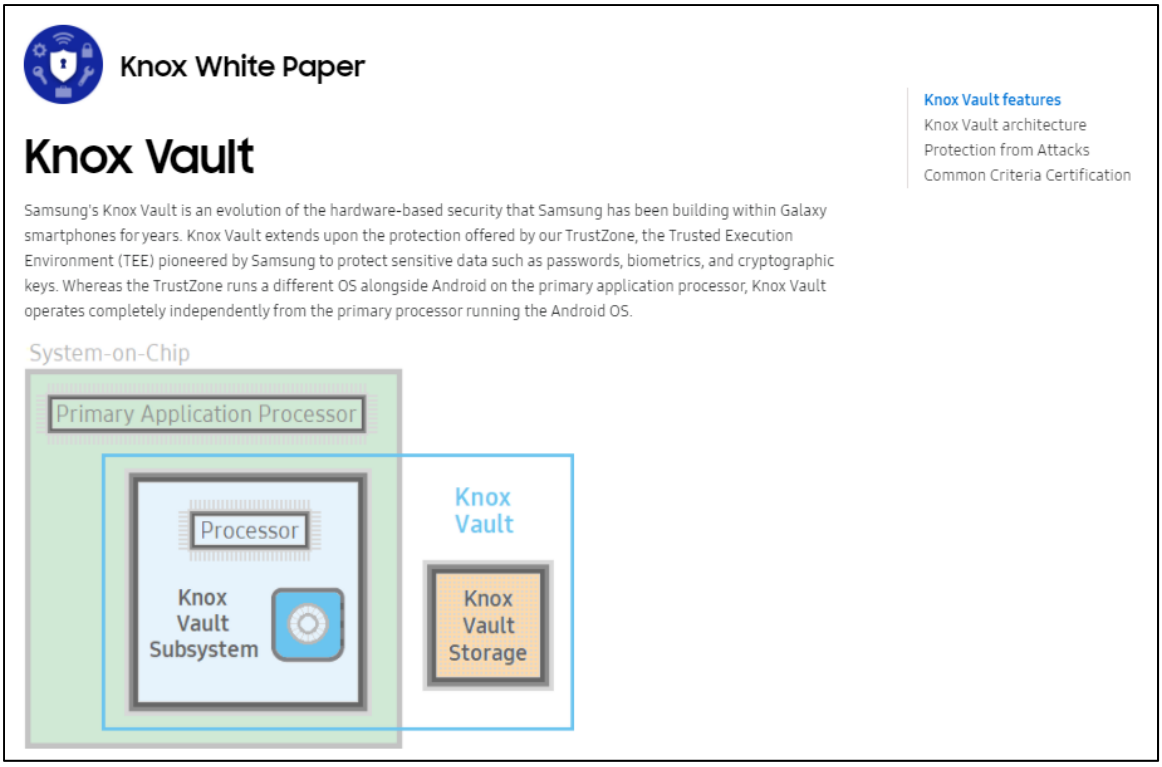
Hamshy Raveendran, *Introducing the Galaxy S21: Supporting Today's Hybrid Workplace*, SAMSUNG INSIGHTS (Jan. 14, 2021), https://insights.samsung.com/2021/01/14/introducing-the-galaxy-s21-supporting-todays-hybrid-workplace/ (last accessed June 17, 2021).

Introducing Samsung Knox Vault

It's a fact that any CISO will accept: isolation increases security. TrustZone is mostly independent, but there remain overlaps and shared resources between the TrustZone and the Android OS. Critically, they share the main CPU and memory, which puts the onus on low-level software protections to keep information isolated. The more we separate sensitive data from the main OS, the more protected they will be in the event of a breach. After all, you are only as secure as your weakest link.

This is where Samsung Knox Vault comes in: a combination of security-specific hardware (a new secure processor and isolated secure memory) and new integrated software that shields your most secure data from the Android OS and applications.

David Thomson, *Understanding Samsung Knox Vault: Protecting the data that matters most*, SAMSUNG NEWSROOM U.S. (Mar. 3, 2021), https://news.samsung.com/us/understanding-samsung-knox-vault-protecting-data-matters-most/.



[. . .]

As a core component of the Knox security platform, Knox Vault is an isolated, tamper-proof, secure subsystem with its own processor and memory, as well as an interface to dedicated, non-volatile secure storage. Knox Vault can:

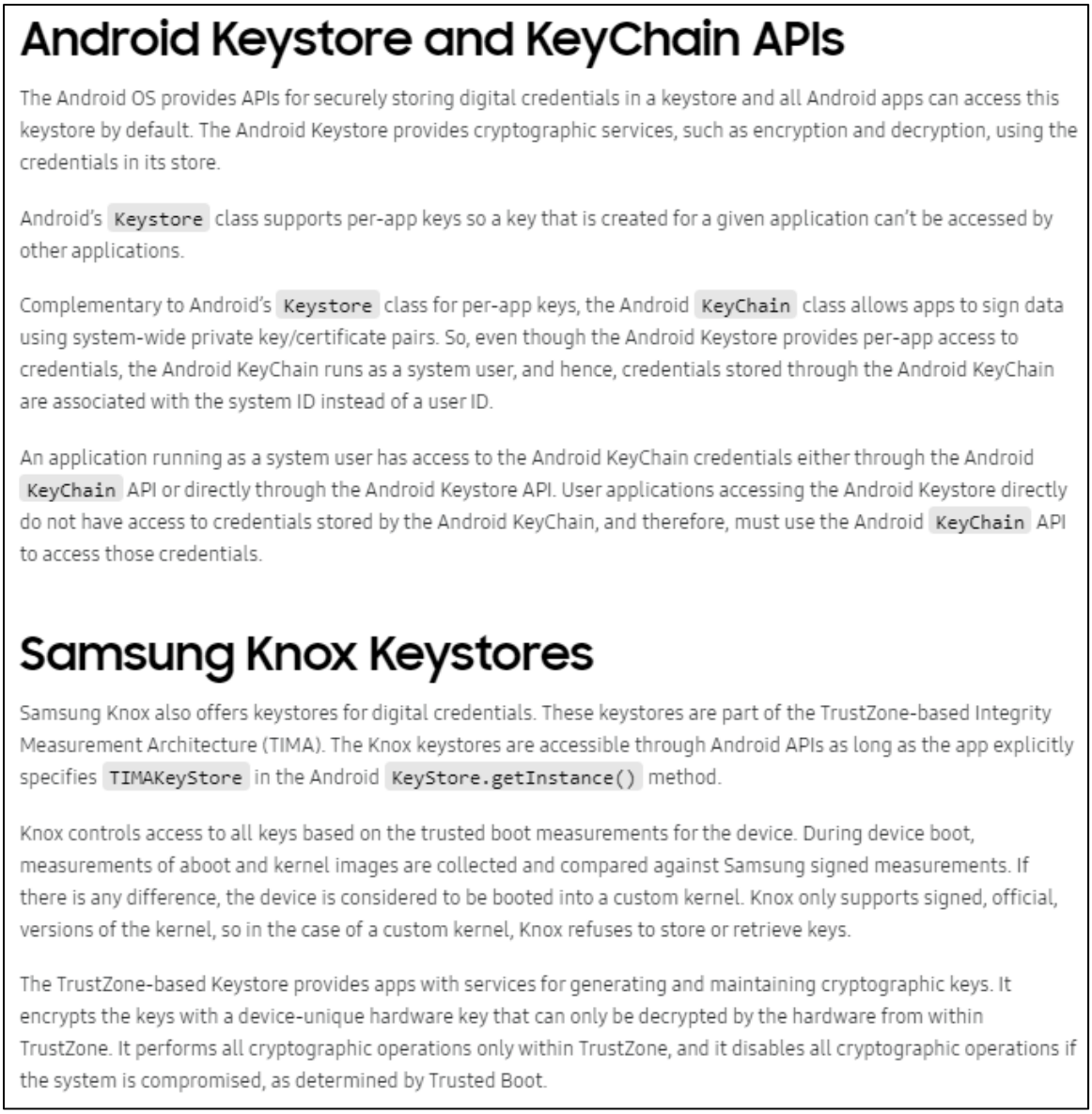
- Store sensitive data such as hardware-backed Android Keystore keys, the Samsung Attestation Key (SAK), biometric data, and blockchain credentials.
- Run security-critical code that authenticates users with increasing timeouts between failures and controls access to keys depending on authentication.

KNOX WHITE PAPER, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

9. Defense-grade Knox security

Samsung has always been at the forefront of mobile device security. The Galaxy S21 is no different, thanks to Samsung Knox, a defense-grade solution for keeping your work and your business protected from the chip up. Knox defends your S21 from intrusions, malware and other malicious threats. The S21 devices also introduce Knox Vault, which combines tamper-resistant secure memory with our secure processor for an additional layer of protection. This advanced security architecture keeps your data — including your Blockchain private key, Samsung Pay credentials and more — out of unauthorized hands.

Michael Archambault, *10 Reasons to Upgrade to the Galaxy S21*, SAMSUNG INSIGHTS (Jan. 14, 2021), https://insights.samsung.com/2021/01/14/10-reasons-to-upgrade-to-the-galaxy-s21/.



Android Keystore and KeyChain APIs

The Android OS provides APIs for securely storing digital credentials in a keystore and all Android apps can access this keystore by default. The Android Keystore provides cryptographic services, such as encryption and decryption, using the credentials in its store.

Android's `Keystore` class supports per-app keys so a key that is created for a given application can't be accessed by other applications.

Complementary to Android's `Keystore` class for per-app keys, the Android `KeyChain` class allows apps to sign data using system-wide private key/certificate pairs. So, even though the Android Keystore provides per-app access to credentials, the Android KeyChain runs as a system user, and hence, credentials stored through the Android KeyChain are associated with the system ID instead of a user ID.

An application running as a system user has access to the Android KeyChain credentials either through the Android `KeyChain` API or directly through the Android Keystore API. User applications accessing the Android Keystore directly do not have access to credentials stored by the Android KeyChain, and therefore, must use the Android `KeyChain` API to access those credentials.

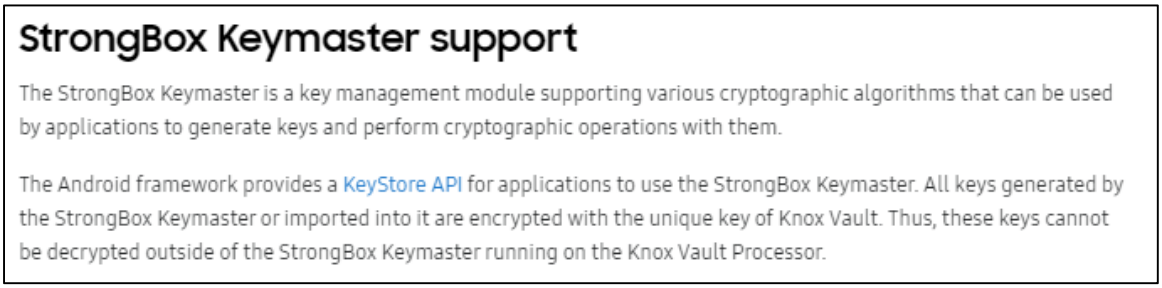
Samsung Knox Keystores

Samsung Knox also offers keystores for digital credentials. These keystores are part of the TrustZone-based Integrity Measurement Architecture (TIMA). The Knox keystores are accessible through Android APIs as long as the app explicitly specifies `TIMAKeyStore` in the Android `KeyStore.getInstance()` method.

Knox controls access to all keys based on the trusted boot measurements for the device. During device boot, measurements of aboot and kernel images are collected and compared against Samsung signed measurements. If there is any difference, the device is considered to be booted into a custom kernel. Knox only supports signed, official, versions of the kernel, so in the case of a custom kernel, Knox refuses to store or retrieve keys.

The TrustZone-based Keystore provides apps with services for generating and maintaining cryptographic keys. It encrypts the keys with a device-unique hardware key that can only be decrypted by the hardware from within TrustZone. It performs all cryptographic operations only within TrustZone, and it disables all cryptographic operations if the system is compromised, as determined by Trusted Boot.

TIMA Keystore, KNOX DEVELOPER DOCUMENTATION: KNOX SDK, https://docs.samsungknox.com/dev/knox-sdk/about-keystores.htm (last accessed June 17, 2021).



StrongBox Keymaster support

The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.

The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

KNOX WHITE PAPER, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

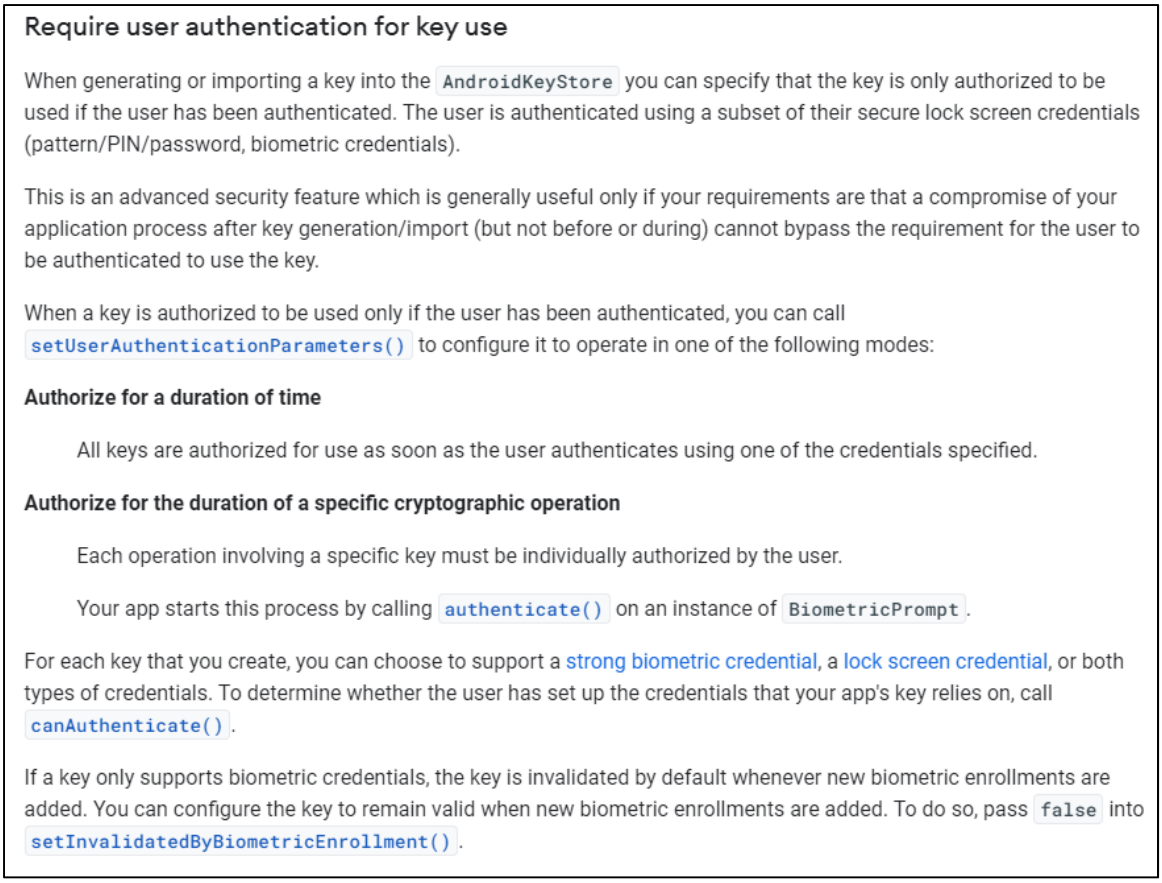
66. The Samsung Accused Products comprise a first processor of a first device configured to: communicate with a second processor using a restricted interface, wherein the second processor is configured to: receive a biometric input from a sensor, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature. This is supported by the exemplary evidence below.

> In the Android OS, fingerprint biometrics are required to be stored in the Trusted Execution Environment (TEE), where the information is encrypted and kept in a separate part of the smartphone, completely inaccessible to the regular OS. It can't even be exported. Android can ask the TEE to verify a user's identity using biometrics, but it can't extract the biometric information. In other words, when the user stores their biometric information, such as a fingerprint, they're not sharing that information outside of their own smartphone or tablet; they're just establishing a way to identify themselves to their device.

[. . .]

> Samsung Pass is an example of a password management service that's based on the FIDO specifications. Samsung Pass enables strong authentication across different apps using biometrics combined with a cloud-based service, provided by Samsung. Smartphone users can lock up multiple sets of authentication credentials — from both public and private enterprise services — and protect them with their fingerprint. Samsung Pass simplifies the user experience while using highly secure authentication systems based on digital certificates, so end users can keep their strong authentication credentials locked up with biometrics, reduce their use of insecure passwords and speed up their app authentication.

Joel Snyder, *Using Biometrics for Authentication in Android*, SAMSUNG INSIGHTS (Apr. 21, 2021), https://insights.samsung.com/2021/04/21/using-biometrics-for-authentication-in-android-2/ (last accessed June 17, 2021).



Require user authentication for key use

When generating or importing a key into the `AndroidKeyStore` you can specify that the key is only authorized to be used if the user has been authenticated. The user is authenticated using a subset of their secure lock screen credentials (pattern/PIN/password, biometric credentials).

This is an advanced security feature which is generally useful only if your requirements are that a compromise of your application process after key generation/import (but not before or during) cannot bypass the requirement for the user to be authenticated to use the key.

When a key is authorized to be used only if the user has been authenticated, you can call `setUserAuthenticationParameters()` to configure it to operate in one of the following modes:

Authorize for a duration of time

All keys are authorized for use as soon as the user authenticates using one of the credentials specified.

Authorize for the duration of a specific cryptographic operation

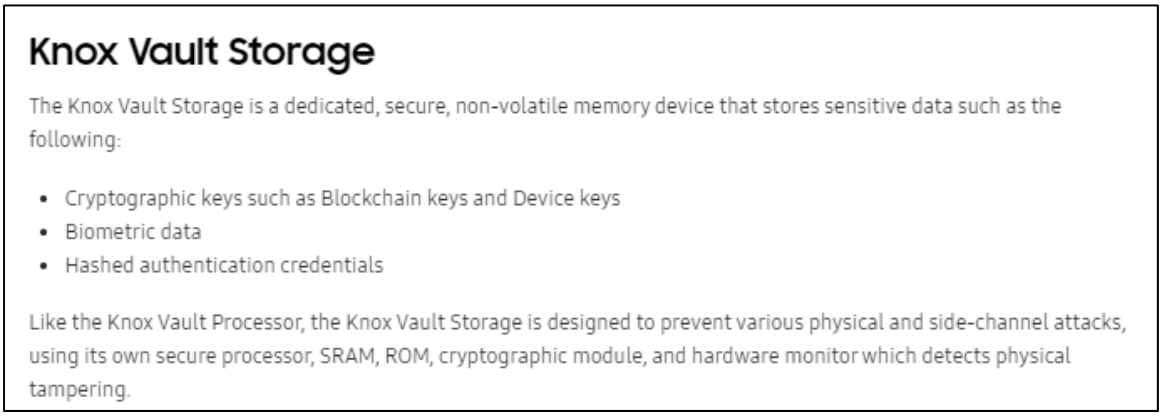
Each operation involving a specific key must be individually authorized by the user.

Your app starts this process by calling `authenticate()` on an instance of `BiometricPrompt`.

For each key that you create, you can choose to support a strong biometric credential, a lock screen credential, or both types of credentials. To determine whether the user has set up the credentials that your app's key relies on, call `canAuthenticate()`.

If a key only supports biometric credentials, the key is invalidated by default whenever new biometric enrollments are added. You can configure the key to remain valid when new biometric enrollments are added. To do so, pass `false` into `setInvalidatedByBiometricEnrollment()`.

Android Keystore System, ANDROID DEVELOPER DOCUMENTATION, https://developer.android.com/training/articles/keystore (last accessed June 17, 2021).



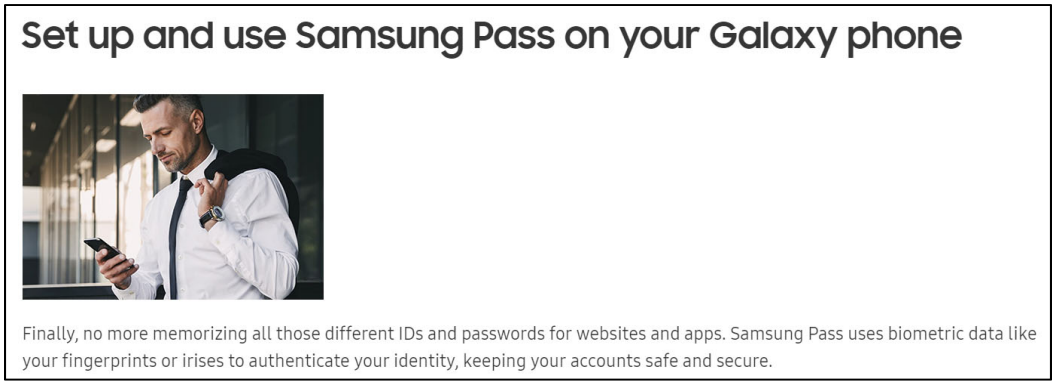
Knox Vault Storage

The Knox Vault Storage is a dedicated, secure, non-volatile memory device that stores sensitive data such as the following:

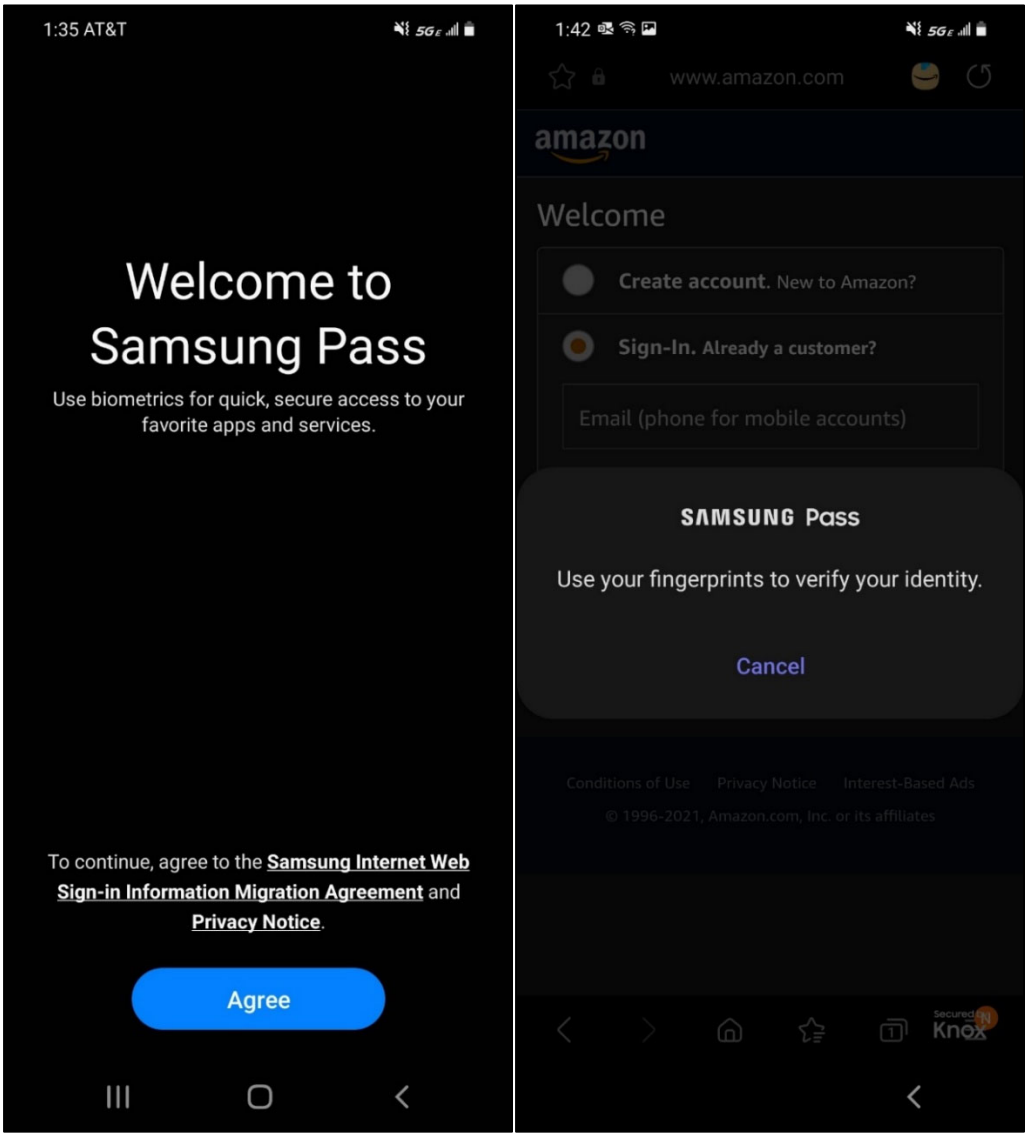
- Cryptographic keys such as Blockchain keys and Device keys
- Biometric data
- Hashed authentication credentials

Like the Knox Vault Processor, the Knox Vault Storage is designed to prevent various physical and side-channel attacks, using its own secure processor, SRAM, ROM, cryptographic module, and hardware monitor which detects physical tampering.

Knox White Paper, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

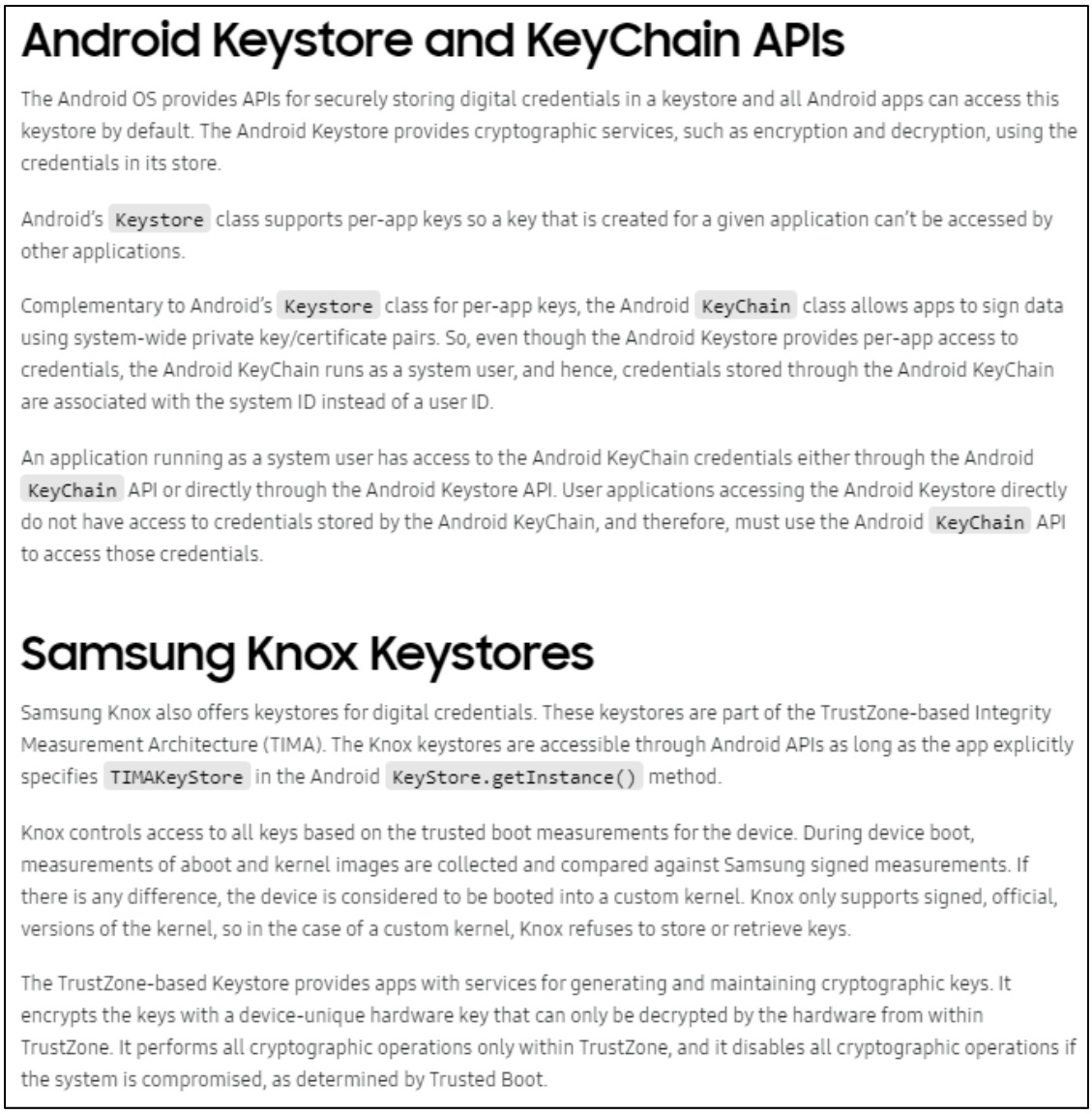


SET UP AND USE SAMSUNG PASS ON YOUR GALAXY PHONE, https://www.samsung.com/us/support/answer/ANS00062705/ (last accessed June 17, 2021).



Screenshots taken on a US-variant Samsung Galaxy S20 mobile phone (taken June 7, 2021).

67. The Samsung Accused Products comprise a first processor of a first device configured to: communicate with a second processor using a restricted interface, wherein the second processor is configured to: access a record stored in a secure storage, wherein the record is associated at least with the external resource and retrieve, from the record, at least one of a password, a cookie, or a cryptographic key. This is supported by the exemplary evidence below.



Android Keystore and KeyChain APIs

The Android OS provides APIs for securely storing digital credentials in a keystore and all Android apps can access this keystore by default. The Android Keystore provides cryptographic services, such as encryption and decryption, using the credentials in its store.

Android's `Keystore` class supports per-app keys so a key that is created for a given application can't be accessed by other applications.

Complementary to Android's `Keystore` class for per-app keys, the Android `KeyChain` class allows apps to sign data using system-wide private key/certificate pairs. So, even though the Android Keystore provides per-app access to credentials, the Android KeyChain runs as a system user, and hence, credentials stored through the Android KeyChain are associated with the system ID instead of a user ID.

An application running as a system user has access to the Android KeyChain credentials either through the Android `KeyChain` API or directly through the Android Keystore API. User applications accessing the Android Keystore directly do not have access to credentials stored by the Android KeyChain, and therefore, must use the Android `KeyChain` API to access those credentials.

Samsung Knox Keystores

Samsung Knox also offers keystores for digital credentials. These keystores are part of the TrustZone-based Integrity Measurement Architecture (TIMA). The Knox keystores are accessible through Android APIs as long as the app explicitly specifies `TIMAKeyStore` in the Android `KeyStore.getInstance()` method.

Knox controls access to all keys based on the trusted boot measurements for the device. During device boot, measurements of aboot and kernel images are collected and compared against Samsung signed measurements. If there is any difference, the device is considered to be booted into a custom kernel. Knox only supports signed, official, versions of the kernel, so in the case of a custom kernel, Knox refuses to store or retrieve keys.

The TrustZone-based Keystore provides apps with services for generating and maintaining cryptographic keys. It encrypts the keys with a device-unique hardware key that can only be decrypted by the hardware from within TrustZone. It performs all cryptographic operations only within TrustZone, and it disables all cryptographic operations if the system is compromised, as determined by Trusted Boot.

TIMA Keystore, KNOX DEVELOPER DOCUMENTATION: KNOX SDK, https://docs.samsungknox.com/dev/knox-sdk/about-keystores.htm (last accessed June 17, 2021).

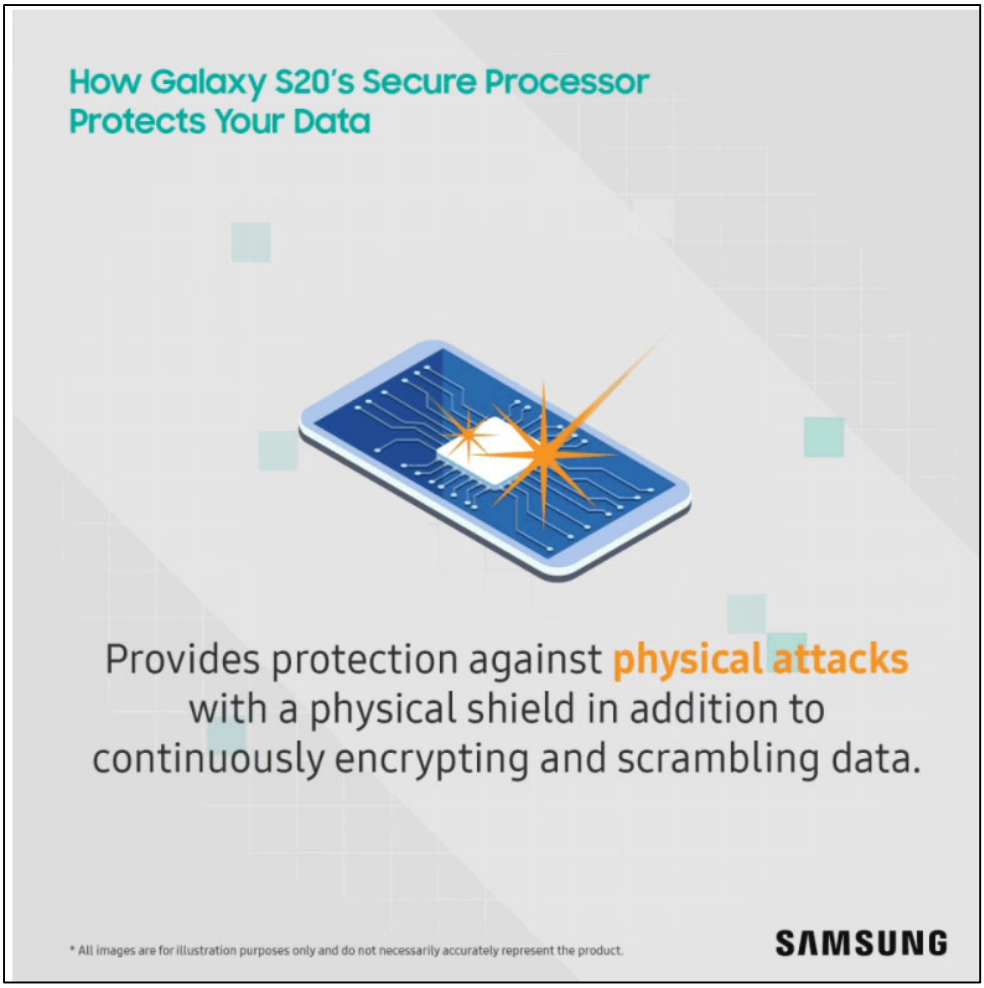
> ***Samsung's new Secure Element solution features secure key storage with CC EAL 5+ certification and dedicated security software for enhanced data protection***
>
> Samsung Electronics, a world leader in advanced semiconductor technology, today introduced a Common Criteria Evaluation Assurance Level (CC EAL) 5+ certified Secure Element (SE) turnkey solution for mobile devices. The new SE offers a strong security solution, consisting of a security chip (S3K250AF) and optimized software, that fully guards private data on an isolated data storage.

[. . .]

> From checking emails and making online payments to replacing house keys and airplane tickets, smart devices continue to offer more applications that enforce stronger security requirements. Samsung's new turnkey solution is a dedicated tamper-resistant strongbox that securely stores users' confidential and cryptographic data such as pin numbers, passwords and even crypto-currency credentials separate from the typical mobile memory such as embedded Universal Flash Storage (eUFS).

Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices, SAMSUNG NEWSROOM (Feb. 26, 2020), https://news.samsung.com/global/samsung-introduces-best-in-class-data-security-chip-solution-for-mobile-devices (last accessed June 17, 2021).

68. The Samsung Accused Products comprise a first processor of a first device configured to: communicate with a second processor using a restricted interface, wherein the second processor is configured to: perform a cryptographic operation. This is supported by the exemplary evidence below.



[. . .]

Enhanced Hardware Security

Just like the way locksmiths can use tools to get past a locked door, malicious actors can manipulate components (physical attacks), provoke hardware errors (fault attacks), or analyze heat and electromagnetic emissions (side-channel attacks) to breach smartphone security. These attacks, also known as hardware attacks, can only happen if the hacker gets hold of the device physically.

The Galaxy S20's secure processor is Samsung's solution to counter against hardware attacks. The component is a physical chip that provides an isolated space to protect confidential data in the device. In addition to the continuous scrambling and encrypting of confidential data, it employs a physical shield to guard against physical attacks. The component can also detect invalid voltage or temperature changes and is equipped with security algorithms to thwart side-channel attacks.

Strengthening Hardware Security with Galaxy S20's Secure Processor, SAMSUNG NEWSROOM (May 15, 2020), https://news.samsung.com/global/strengthening-hardware-security-with-galaxy-s20s-secure-processor (last accessed June 17, 2021).

> Knox Vault is integrated into Samsung devices starting from the Galaxy S21, and is comprised of components that are Common Criteria evaluated to the requirements in BSI PP0084 at EAL4+ or higher. These components are tested by an independent lab against a wide array of hardware attacks and through a review of their software and firmware.

[. . .]

> **StrongBox Keymaster support**
>
> The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.
>
> The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

[. . .]

> **Crypto engine**
>
> A hardware cryptographic module provides the following cryptographic functions:
>
> - AES encryption/decryption
> - DRBG random number generation
> - SHA hashing
> - HMAC keyed-hashing for message authentication code
> - RSA and ECC key generation and services

KNOX WHITE PAPER, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

69. The Samsung Accused Products comprise a first processor of a first device configured to: communicate with a second processor using a restricted interface, wherein the second processor is configured to: in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output. This is supported by the exemplary evidence below.

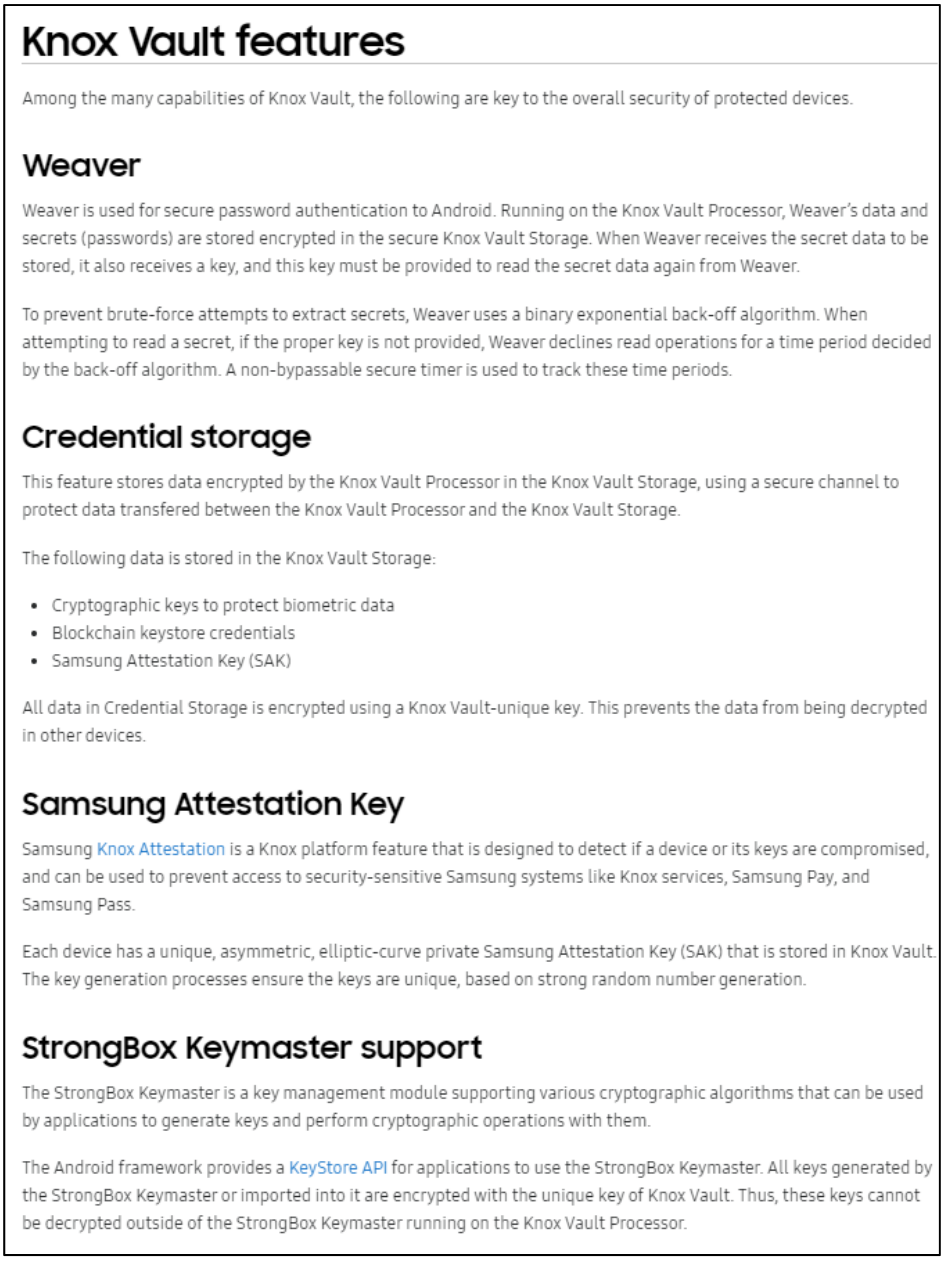
Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices

Korea on February 26, 2020 Audio Share

[. . .]

From checking emails and making online payments to replacing house keys and airplane tickets, smart devices continue to offer more applications that enforce stronger security requirements. Samsung's new turnkey solution is a dedicated tamper-resistant strongbox that securely stores users' confidential and cryptographic data such as pin numbers, passwords and even crypto-currency credentials separate from the typical mobile memory such as embedded Universal Flash Storage (eUFS).

Samsung Introduces Best-in-Class Data Security Chip Solution for Mobile Devices, SAMSUNG NEWSROOM (Feb. 26, 2020), https://news.samsung.com/global/samsung-introduces-best-in-class-data-security-chip-solution-for-mobile-devices (last accessed June 17, 2021).



Knox Vault features

Among the many capabilities of Knox Vault, the following are key to the overall security of protected devices.

Weaver

Weaver is used for secure password authentication to Android. Running on the Knox Vault Processor, Weaver's data and secrets (passwords) are stored encrypted in the secure Knox Vault Storage. When Weaver receives the secret data to be stored, it also receives a key, and this key must be provided to read the secret data again from Weaver.

To prevent brute-force attempts to extract secrets, Weaver uses a binary exponential back-off algorithm. When attempting to read a secret, if the proper key is not provided, Weaver declines read operations for a time period decided by the back-off algorithm. A non-bypassable secure timer is used to track these time periods.

Credential storage

This feature stores data encrypted by the Knox Vault Processor in the Knox Vault Storage, using a secure channel to protect data transfered between the Knox Vault Processor and the Knox Vault Storage.

The following data is stored in the Knox Vault Storage:

- Cryptographic keys to protect biometric data
- Blockchain keystore credentials
- Samsung Attestation Key (SAK)

All data in Credential Storage is encrypted using a Knox Vault-unique key. This prevents the data from being decrypted in other devices.

Samsung Attestation Key

Samsung Knox Attestation is a Knox platform feature that is designed to detect if a device or its keys are compromised, and can be used to prevent access to security-sensitive Samsung systems like Knox services, Samsung Pay, and Samsung Pass.

Each device has a unique, asymmetric, elliptic-curve private Samsung Attestation Key (SAK) that is stored in Knox Vault. The key generation processes ensure the keys are unique, based on strong random number generation.

StrongBox Keymaster support

The StrongBox Keymaster is a key management module supporting various cryptographic algorithms that can be used by applications to generate keys and perform cryptographic operations with them.

The Android framework provides a KeyStore API for applications to use the StrongBox Keymaster. All keys generated by the StrongBox Keymaster or imported into it are encrypted with the unique key of Knox Vault. Thus, these keys cannot be decrypted outside of the StrongBox Keymaster running on the Knox Vault Processor.

KNOX WHITE PAPER, https://docs.samsungknox.com/admin/whitepaper/kpe/knox-vault.htm (last accessed June 17, 2021).

SECURITY TIPS

Using biometrics for authentication in Android

Published Apr 21, 2021 By: Joel Snyder

To unlock their mobile devices more simply, users are now favoring biometric authentication, such as fingerprint sensors, which also reduce the cognitive burden of remembering multiple long passwords.

Proper use of biometrics increases security, too. Passwords are easy to steal; faking biometrics is much more difficult. The technology is ideal for providing role-based access controls — and a high level of trust for business users.

Here's a detailed look at how biometrics work, how data encryption fits in and what business leaders should look for to maintain strong security while delivering the convenience users want:

How biometrics work

Unlike passwords or PINs, biometrics aren't saved in the network or passed around between devices and servers. Instead, biometrics protect other authentication information — usually a digital certificate or private key — and it's this protected information that is actually used to verify the user.

[. . .]

In the Android OS, fingerprint biometrics are required to be stored in the Trusted Execution Environment (TEE), where the information is encrypted and kept in a separate part of the smartphone, completely inaccessible to the regular OS. It can't even be exported. Android can ask the TEE to verify a user's identity using biometrics, but it can't extract the biometric information. In other words, when the user stores their biometric information, such as a fingerprint, they're not sharing that information outside of their own smartphone or tablet; they're just establishing a way to identify themselves to their device.

Joel Snyder, *Using Biometrics for Authentication in Android*, SAMSUNG INSIGHTS (Apr. 21, 2021), https://insights.samsung.com/2021/04/21/using-biometrics-for-authentication-in-android-2/ (last accessed June 7, 2021).

Set up and use Samsung Pass on your Galaxy phone

Finally, no more memorizing all those different IDs and passwords for websites and apps. Samsung Pass uses biometric data like your fingerprints or irises to authenticate your identity, keeping your accounts safe and secure.

SET UP AND USE SAMSUNG PASS ON YOUR GALAXY PHONE, https://www.samsung.com/us/support/answer/ANS00062705/ (last accessed June 17, 2021).

70. The Samsung Accused Products comprise a first processor of a first device configured to: communicate with a second processor using a restricted interface, wherein the second processor is configured to: perform a secure backup of the record to a storage service, wherein a second device associated with the user is registered with the storage service, and wherein the record is downloaded from the storage service by the second device. This is supported by the exemplary evidence below.

> **2. Samsung Pass Features**
>
> 2.1 Samsung Pass is a biometric authentication solution which enables users to sign in to websites on Samsung Internet as well as Samsung and third-party mobile applications or websites that have enabled Samsung Pass functionality (a "Third-Party Service") by using a user's stored biometric information. Instead of manually entering your username and password into a Samsung or Third-Party Service each time you wish to access your account with such Samsung or Third-Party Service, Samsung Pass acts as a central repository of your log-in and biometric information for authentication purposes. Samsung Pass may also be used to pre-populate certain forms and applications and to remotely log you in to certain Samsung and Third-Party Services accessed through a PC web browser.

[. . .]

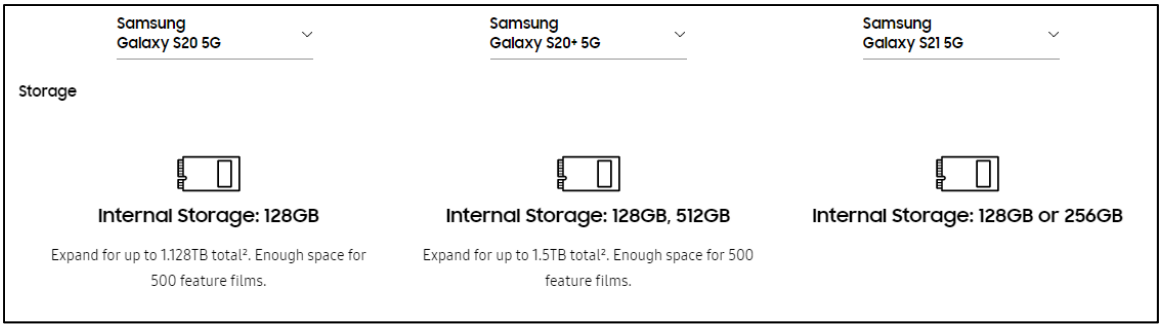
> 2.4 You may use your Samsung Pass account across multiple Samsung devices, the number of which may be limited or changed in Samsung's sole discretion. Deleting your biometric information from your mobile device will make your Samsung Pass account dormant, but will not automatically cancel your Samsung Pass account. You can reactivate your dormant Samsung Pass account by re-entering your biometric information and your Samsung Account password on your mobile device.
>
> 2.5 You can delete the Samsung Pass data stored on your device and reset Samsung Pass to its default settings by selecting "Delete data" on the Samsung Pass settings menu or selecting "Reset" on this website. Please note that doing so will not delete certain Samsung Pass data that Samsung has collected on its servers.

SAMSUNG PASS SUPPLEMENTARY TERMS OF SERVICE (June 21, 2019), https://account.samsung.com/membership/etc/specialTC.do?fileName=samsungpass.html (last accessed June 17, 2021).

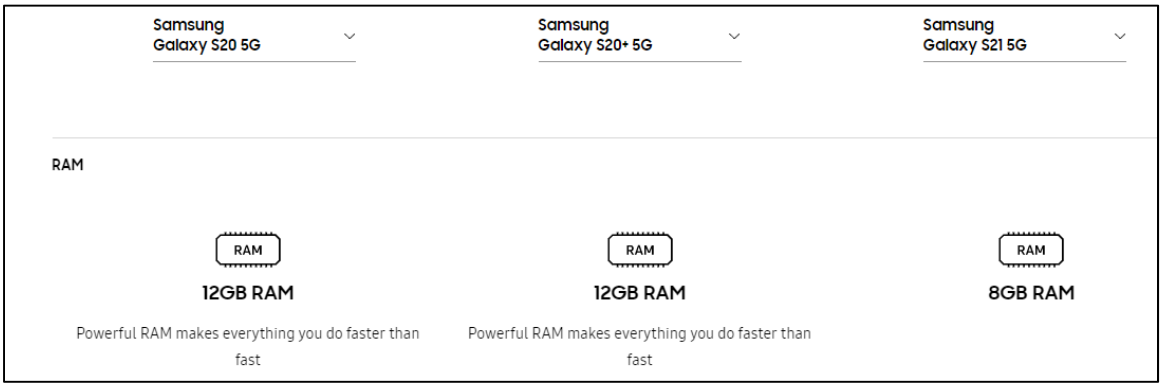
> **Can I use Samsung Pass on multiple devices?**
>
> You can use Samsung Pass seamlessly on up to 5 mobile devices. Using the same Samsung account in your new or additional devices will sync your saved website list and ID/passwords. However, you need to register your fingerprints on each device.

GENERAL QUESTIONS AND INFORMATION ABOUT SAMSUNG PASS, https://www.samsung.com/us/support/answer/ANS00066601/ (last accessed June 17, 2021); *see also* SAMSUNG PASS FAQS FOR THE PHONE, https://www.samsung.com/us/support/troubleshooting/TSG01001481/ (last accessed June 17, 2021).

71. The Samsung Accused Products comprise a memory coupled to the first processor and configured to provide the first processor with instructions. This is supported by the exemplary evidence below.



[. . .]



HOW THE SAMSUNG S20 FE 5G COMPARES, https://www.samsung.com/us/mobile/galaxy-s20-5g/compare/?device-1=samsung-galaxy-s20-5g&device-2=samsung-galaxy-s20%2B-5g&device-3=samsung-galaxy-s21-5g (last accessed June 17, 2021).

72. Samsung also indirectly infringes claims of the '512 Patent, as provided in 35 U.S.C. § 271(b), by inducing infringement by others, such as Samsung's customers and end users, in this District and elsewhere in the United States. For example, Samsung's customers and end users directly infringe through their use of the inventions claimed in the '512 Patent. Samsung induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products and related services, and providing instructions, documentation, online technical support, marketing, product manuals, advertisements, and other information to customers and end users suggesting they use the Accused Products and related services in an infringing manner. As a result of Samsung's inducement, Samsung's customers and end users use the Accused Products and related services in the way Samsung intends and directly infringe the '512 Patent.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

73. A judgment in favor of RightQuestion that Samsung has infringed, directly and indirectly, by way of inducement and/or contributory infringement, literally and/or under the doctrine of equivalents, the patents-in-suit;

74. An award of damages to which RightQuestion is entitled under 35 U.S.C. § 284 and 35 U.S.C. § 154(d) for Samsung's past infringement and any continuing or infringement post-trial up until the date a final judgment is entered, including both compensatory damages and treble damages for willful infringement;

75. RightQuestion's actual damages in an amount sufficient to compensate RightQuestion for Samsung's infringement of the patents-in-suit until such time as Samsung ceases its infringing conduct, including supplemental damages post-verdict;

76. A judgment and order against Samsung for exemplary damages as determined by the trier of fact;

77. A judgment that Samsung's infringement has been willful;

78. Pre- and post-judgment interest as allowed by law on any damages awarded to RightQuestion;

79. A judgment and order requiring Samsung to pay the costs of this action (including all disbursements), as well as attorneys' fees as provided by 35 U.S.C. § 285;

80. A judgment and order requiring Samsung to pay RightQuestion compulsory ongoing licensing fees, as determined by the Court in equity; and

81. Such other and further relief in law or in equity to which RightQuestion may be justly entitled.

DEMAND FOR JURY TRIAL

RightQuestion demands a trial by jury of any and all issues triable of right before a jury, except for future patent infringement, which is an issue in equity to be determined by the Court.

Dated: June 29, 2021

MCKOOL SMITH, P.C.

/s/ Joshua W. Budwin

Joshua W. Budwin
Lead Attorney
Texas State Bar No. 24050347
jbudwin@mckoolsmith.com
R. Mitch Verboncoeur
Texas State Bar No. 24105732
mverboncoeur@mckoolsmith.com
George T. Fishback, Jr.
Texas State Bar No. 24120823
gfishback@McKoolSmith.com
MCKOOL SMITH, P.C.
303 Colorado, Suite 2100
Austin, Texas 78701
Telephone: (512) 692-8700
Telecopier: (512) 692-8744

Richard A. Kamprath
Texas State Bar No. 24078767
rkamprath@mckoolsmith.com
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Telephone: (214) 978-4000
Facsimile: (214) 978-4044

ATTORNEYS FOR PLAINTIFF RIGHTQUESTION, LLC